UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS BLUMENAU
LICENCIATURA EM MATEMÁTICA

Camila Ignaczuk Lima

Sequências exatas de grupos

Blumenau
2021

Camila Ignaczuk Lima

Sequências exatas de grupos

Trabalho de Conclusão de Curso de Graduação em Licenciatura em Matemática do Campus Blumenau da Universidade Federal de Santa Catarina para a obtenção do título de Licenciado(a) em Matemática.
Orientador: Prof. Dr. Felipe Vieira

Blumenau
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Ignaczuk Lima, Camila
Sequências exatas de grupos / Camila Ignaczuk Lima ; orientador, Felipe Vieira , 2021.
91 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Blumenau, Graduação em Matemática, Blumenau, 2021.

Inclui referências.

1. Matemática. 2. Álgebra. 3. Grupos. 4. Sequências exatas de grupos . I. Vieira , Felipe. II. Universidade Federal de Santa Catarina. Graduação em Matemática. III. Título.

Camila Ignaczuk Lima

Sequências exatas de grupos

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado(a) em Matemática e aprovado em sua forma final pelo Curso de Licenciatura em Matemática.

Blumenau, 13 de Maio de 2021.

Documento assinado digitalmente
Julio Faria Correa
Data: 24/05/2021 14:07:34-0300
CPF: 045.818.289-37
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Júlio Faria Corrêa
Coordenador do Curso

Banca Examinadora:

Documento assinado digitalmente
Felipe Vieira
Data: 24/05/2021 10:04:34-0300
CPF: 009.601.639-64
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Felipe Vieira
Orientador
Universidade Federal de Santa Catarina - UFSC

Prof[a]. Dr[a]. Naiara Vergian de Paulo Costa
Avaliadora
Universidade Federal de Santa Catarina - UFSC

Prof. Dr. Renan Gambale Romano
Avaliador
Universidade Federal de Santa Catarina - UFSC

Para todos aqueles que gostam de álgebra.

AGRADECIMENTOS

Gostaria de agradecer a todos que de alguma forma fizeram parte da minha trajetória acadêmica.

Aos meus professores, que fizeram toda a diferença na minha formação. Em especial, para o meu orientador, que foi um excelente mentor e teve muita paciência durante todo esse processo. Agradeço também às professoras Louise e Naiara, que são mulheres e matemáticas inspiradoras. Quando eu crescer eu quero ser como vocês.

Aos amigos que eu fiz durante a graduação, por todo o apoio, conversas, grupos de estudos e cafés. Pelas inúmeras listas de exercícios resolvidas. Com vocês tudo ficou mais suportável. Um agradecimento especial ao amigo Gustavo, pela parceria nessa jornada.

Agradeço minha mãe e minha irmã, que sempre me apoiaram.

Ao meu companheiro Fábio, por acreditar em mim, mesmo quando eu falhava neste quesito.

A minha amiga Cíntia, certamente uma das melhores coisas de ter estudado na UFSC foi ter conhecido você.

Finalmente, meu maior agradecimento vai para aqueles que lutaram e aqueles que lutam por uma educação pública, gratuita e de qualidade.

"The beauty of mathematics only shows itself to more patient followers."
(Maryam Mirzakhani, 2008)

RESUMO

Este trabalho tem como objetivo apresentar o tema sequências exatas de grupos. Para isto, inicialmente discutiremos sobre os aspectos da teoria de grupos que são necessários para o estudo de tal conteúdo. Em seguida, após o embasamento mencionado, estudaremos as características das sequências exatas e demonstraremos dois teoremas relevantes sobre o assunto.

Palavras-chave: Grupos. Produto direto. Produto semidireto. Sequências exatas.

ABSTRACT

This work aims to present the theme of exact group sequences. For this, we will initially discuss the aspects of group theory that are necessary for the study of such content. Then, we will study the characteristics of the exact sequences and prove two relevant theorems on the subject.

Keywords: Groups. Direct product. Semidirect product. Exact sequences.

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A teoria de grupos faz parte da matemática desde meados do século XVIII, onde primórdios desta teoria foram estudados por Leonard Euler (1707-1783), Évariste Galois (1811-1832), Paolo Ruffini (1765-1822), Augustin-Louis Cauchy (1789-1857), entre outros. Apenas no ano de 1893 que o matemático alemão Heinrich Weber (1842-1913) apresentou uma definição formal para grupos. A primeira publicação em inglês sobre o assunto aconteceu em 1897, pelo matemático inglês William Burnside (1852-1927).

Neste trabalho, o leitor poderá conhecer alguns dos tópicos da teoria de grupos. Estes princípios servirão de embasamento para o estudo das *sequências exatas de grupos*. Para a fundamentação de tal teoria, o primeiro capítulo é dedicado exclusivamente para estes resultados. Vamos apresentar como será a organização do trabalho.

O Capítulo 2 inicia com a definição de grupo, e a partir desta definição algumas propriedades de grupos serão deduzidas. Ao longo deste capítulo, serão apresentados os conceitos de subgrupo, subgrupos normais e grupo quociente, assim como exemplos. No mesmo capítulo, falaremos sobre homomorfismos. Homomorfismo (do grego, *mesmo formato)* é uma concepção importantíssima na teoria de grupos, pois ele preserva estruturas algébricas, permitindo que encontremos relações diversas entre grupos. No final do capítulo o leitor encontrará uma construção intuitiva do produto semidireto e o capítulo finaliza com dois exemplos partindo desta ideia. Este capítulo foi baseado nas referências [2], [4] e [5].

No Capítulo 3, todos os conceitos apresentados no Capítulo 2 são utilizados para o estudo das sequências exatas de grupos. Sequências exatas de grupos são sequências formadas por grupos e homomorfismos, e para cada homomorfismo α_i que faz parte da sequência,

temos que $Ker(\alpha_i) = Im(\alpha_{i-1})$. O objetivo principal deste trabalho é a demonstração de dois teoremas. O primeiro, nos dará condições para saber quando que a partir de uma sequência exata de grupos é possível construir uma nova sequência exata que é isomorfa a esta primeira, onde a sequência obtida envolve o produto direto de dois grupos da primeira sequência. Por se tratarem de estruturas algébricas, lidamos com elementos abstratos. Mesmo não tendo conhecimento de quem são exatamente esses elementos, o segundo teorema, assim como o primeiro, nos apresentará as condições necessárias para que uma nova sequência exata seja obtida, onde esta segunda poderá ser escrita usando o produto semidireto de dois grupos da sequência exata inicial. Estes teoremas são muito relevantes, pois nem sempre é trivial encontrar um isomorfismo entre dois grupos. Além do mais, "criar" um produto semidireto muitas vezes não é uma tarefa simples. Para a construção deste capítulo, a referência [1] foi a mais utilizada.

O presente trabalho não é totalmente autocontido, visto que algumas demonstrações não estarão explicitadas em seu conteúdo. Quando isto acontecer, o leitor encontrará referências dos resultados.

Por fim, acreditamos que o assunto deste trabalho pode ser compreendido por qualquer pessoa que já tenha algum contato com os aspectos básicos da teoria de anéis e com a matemática do ensino superior e suas formalidades.

2 GRUPOS

Neste primeiro capítulo serão abordados os tópicos preliminares da teoria de grupos que são necessários para a construção de sequências exatas de grupos. Primeiro, vamos saber o que é um grupo.

Definição 2.1. Um grupo é um par ordenado $(G, \cdot)$ onde G é um conjunto e $\cdot$ é uma operação binária fechada satisfazendo as seguintes propriedades:

1. Associatividade:

$$\forall\, g, h, k \in G, (g \cdot h) \cdot k = g \cdot (h \cdot k)$$

2. Existência do elemento neutro:

$$\exists\, 1 \in G : \forall\, g \in G, g \cdot 1 = 1 \cdot g = g$$

3. Existência do elemento inverso:

$$\forall\, g \in G,\ \exists\, h \in G : g \cdot h = h \cdot g = 1$$

Observação 2.1. *O conjunto vazio não é um grupo, uma vez que isso contradiria a Propriedade 2.*

Definição 2.2. Seja $(G, \cdot)$ um grupo. Se a operação $\cdot$ for comutativa, o grupo é dito abeliano.

No decorrer deste trabalho, denotaremos um grupo somente por G, e a operação entre elementos deste grupo será representada pela notação multiplicativa usual. Da mesma forma, o elemento neutro muitas vezes será representado pelo símbolo 1, mesmo que não saibamos a natureza do grupo. Em outros momentos, a operação será explicitada assim como o elemento neutro.

Algumas proposições podem ser verificadas a partir da definição de grupos.

Proposição 2.1. O elemento neutro de um grupo é único.

Demonstração. De fato, considere g e h elementos neutros de G. Pela Propriedade 3 da definição de grupos, temos que

$$g = g \cdot h = h \implies g = h$$

ou seja, o elemento neutro é único. □

Proposição 2.2. O elemento inverso de um grupo é único.

Demonstração. Sejam g, h e $k \in G$. Suponha que h e k sejam inversos de g. Assim, pela Proposição 3 da definição de grupos, $g \cdot h = 1$ e $k \cdot g = 1$. Então,

$$k = k \cdot 1 = k \cdot (g \cdot h) = (k \cdot g) \cdot h = 1 \cdot h = h$$

Logo, $k = h$. Portanto, o inverso de um elemento é único. □

A partir deste ponto, vamos denotar o inverso de um elemento qualquer $g \in G$ por g^{-1}.

Proposição 2.3. Dado $g \in G$, $(g^{-1})^{-1} = g$.

Demonstração. Se $g \in G$ então $g^{-1} \in G$. Pela Propriedade 3 da definição de grupos, segue que

$$g^{-1} \cdot g = g \cdot g^{-1} = 1$$

Pela unicidade do inverso, conclui-se que $(g^{-1})^{-1} = g$. □

Proposição 2.4. Dados $g, h \in G$, $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

Demonstração. Considere $k = (g \cdot h)^{-1}$, então

$$\begin{aligned} k \cdot (g \cdot h) &= 1 \\ \implies k \cdot (g \cdot h) \cdot h^{-1} &= 1 \cdot h^{-1} \\ \implies k \cdot g \cdot (h \cdot h^{-1}) &= h^{-1} \\ \implies k \cdot g &= h^{-1} \\ \implies k \cdot g \cdot g^{-1} &= h^{-1} \cdot g^{-1} \\ \implies k &= h^{-1} \cdot g^{-1} \end{aligned}$$

Logo, $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$. □

Sabemos que o conjunto dos números reais tem a propriedade associativa. Neste trabalho não demonstraremos tal fato, mas usaremos esta propriedade para exibir grupos envolvendo os números reais, assim como números complexos, racionais e inteiros. Iremos explorar alguns exemplos de grupos nas próximas páginas. Para mostrar que determinado conjunto e operação configuram um grupo, basta verificar se as três propriedades da Definição 2.1 são satisfeitas.

Exemplo 2.1. O conjunto dos números inteiros com a adição usual é um grupo. De fato, sabemos que a adição de números inteiros é associativa, e a primeira propriedade está satisfeita. Ainda, com a adição usual, temos que

$$0 + a = a + 0 = a, \ \forall \ a \in \mathbb{Z}$$

Portanto, 0 é o elemento neutro. Para qualquer $a \in \mathbb{Z}$, existe $-a$ inteiro, de modo que

$$(-a) + a = a + (-a) = 0$$

Desta forma, podemos formar o grupo aditivo dos inteiros $(\mathbb{Z}, +)$.

Exemplo 2.2. Sejam $a, b, c, d \in \mathbb{Z}$, com $b, d \neq 0$. Defina o conjunto dos números racionais

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

A soma de dois números racionais é caracterizada por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Vamos mostrar que $(\mathbb{Q}, +)$ é um grupo. A soma definida acima é associativa, pois, dados $a, b, c, d, e, f \in \mathbb{Z}$, com $b, d, f \neq 0$, usando o fato de que $\mathbb{Z}$ é um grupo, segue que

$$\begin{aligned}
\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} &= \frac{ad + bc}{bd} + \frac{e}{f} \\
&= \frac{f(ad + bc) + ebd}{bdf} \\
&= \frac{fad + fbc + ebd}{bdf} \\
&= \frac{adf + bcf + bde}{bdf} \\
&= \frac{adf + b(cf + de)}{bdf} \\
&= \frac{a}{b} + \frac{cf + de}{df} \\
&= \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)
\end{aligned}$$

O elemento neutro deste grupo é $\frac{0}{1}$, e para qualquer $\frac{a}{b} \in \mathbb{Q}$, existe um oposto $\frac{-a}{b} \in \mathbb{Q}$ de modo que a Propriedade 3 se verifica. Logo, todas as propriedades de grupo são cumpridas.

Exemplo 2.3. Grupo aditivo dos complexos $(\mathbb{C}, +)$. Considere o conjunto dos números complexos

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

com a operação

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

Vamos verificar se a soma destes elementos é associativa:

$$\begin{aligned} a+bi+(c+di+e+fi) &= a+bi+(c+e+(d+f)i) \\ &= a+c+e+(b+d+f)i \\ &= a+c+(b+d)i+e+fi \\ &= (a+bi+c+di)+e+fi \end{aligned}$$

Como o elemento neutro deste grupo é $0+0i$, o oposto de um número complexo é $(-a)+(-b)i$ uma vez que

$$(a+bi)+((-a)+(-b)i)=((-a)+(-b)i)+(a+bi)=0+0i$$

Ao tentar definir um grupo numérico usando a multiplicação usual, é preciso se atentar ao fato de que 0 não possui inverso nesta operação, logo, precisamos excluí-lo para formar um grupo. De um modo geral, temos que os conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ são grupos multiplicativos. Para cada um deles, o elemento neutro é o número 1, e o inverso multiplicativo de um a qualquer é $\frac{1}{a}$.

Exemplo 2.4. Grupo aditivo das matrizes $m \times n$ ($M_{m\times n}(K)$), onde K pode ser $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
A soma de duas matrizes $m \times n$ resulta em uma matriz $m \times n$, e a soma de matrizes é associativa. O elemento neutro neste grupo é a matriz nula, que é formada pelo número 0 em todas as posições, e dado $M \in M_{m\times n}(K)$,

$$M=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},$$

o elemento inverso será

$$M^{-1} = \begin{bmatrix} -a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & -a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m1} & -a_{m2} & \cdots & -a_{mn} \end{bmatrix}$$

Exemplo 2.5. Seja A um anel com unidade multiplicativa e A^* o conjunto dos elementos inversíveis de A. Então $(A^*, \cdot)$ é um grupo, e será abeliano se A for comutativo.
Como A é um anel, temos que a Propriedade 1 é satisfeita. Ainda, para qualquer $a \in (A^*, \cdot)$ temos que $a^{-1} \in (A^*, \cdot)$ e $a \cdot a^{-1} = 1$, que é o elemento neutro da multiplicação. Logo, $(A^*, \cdot)$ é um grupo. Em particular, esta é outra forma de ver que $\mathbb{R}^*$ é um grupo.

O leitor pode encontrar a definição e exemplos de anéis no Capítulo 3 de [5].

Exemplo 2.6. Sejam $(G, *)$ e $(H, \cdot)$ grupos. Pode-se formar um novo grupo $(G \times H, \bullet)$ denominado produto direto, onde

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$$

Do fato que G e H são grupos, temos que individualmente eles satisfazem todas as propriedades de grupo. A partir do momento que tentamos criar um novo grupo a partir de dois grupos existentes, é necessário verificar se esta nova operação está alinhada com aquelas propriedades.
Note que o elemento neutro de $(G \times H, \bullet)$ será $(1_G, 1_H)$, onde 1_G e 1_H são os elementos neutros de G e H, respectivamente.

Sejam $g_1, g_2, g_3 \in G$ e $h_1, h_2, h_3 \in H$.

$$\begin{aligned}(g_1, h_1) \bullet [(g_2, h_2) \bullet (g_3, h_3)] &= (g_1, h_1) \bullet (g_2 * g_3, h_2 \cdot h_3) \\ &= (g_1 * g_2 * g_3, h_1 \cdot h_2 \cdot h_3) \\ &= (g_1 * g_2, h_1 \cdot h_2) \bullet (g_3, h_3) \\ &= [(g_1, h_1) \bullet (g_2, h_2)] \bullet (g_3, h_3)\end{aligned}$$

Logo, a operação é associativa.
Para cada $(g, h) \in G \times H$, seu elemento inverso será:

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

pois

$$(g, h) \bullet (g^{-1}, h^{-1}) = (g * g^{-1}, h \cdot h^{-1}) = (1_G, 1_H)$$

Logo, a operação $\bullet$ satisfaz as propriedades e $(G \times H, \bullet)$ é um grupo.

Vamos exemplificar esta situação, descrevendo o produto direto de $\mathbb{Z}_2$ com $\mathbb{Z}_3$:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \big\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\big\}$$

Exemplo 2.7. O conjunto $\mathbb{Z}_n = \big\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\big\}$, das classes residuais módulo n é um grupo abeliano aditivo, com a operação de soma

$$\overline{x} + \overline{y} = \overline{x + y}$$

em que, caso $x + y > n - 1$, $\overline{x + y}$ deve ser entendido como $\overline{x + y - n}$. O elemento neutro deste grupo é $\overline{0}$, e para cada elemento $x \in \mathbb{Z}_n$ seu inverso será

$$\overline{x}^{-1} = \overline{n + (-x)}$$

Os próximos exemplos exploram grupos não abelianos, clássicos da teoria de grupos.

Exemplo 2.8. Seja $GL_2(\mathbb{R})$ o conjunto das matrizes 2×2 inversíveis com coeficientes reais. Mostraremos que este conjunto munido da multiplicação é um grupo. Primeiramente, se multiplicarmos dois elementos quaisquer em $GL_2(\mathbb{R})$ o elemento resultante será um elemento de $GL_2(\mathbb{R})$, logo, o conjunto é fechado para a operação. A operação é associativa, pois

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \right] \begin{pmatrix} j & k \\ m & n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} j & k \\ m & n \end{pmatrix} \right]$$

O elemento neutro é

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e ainda,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{-d}{bc-ad} & \frac{b}{bc-ad} \\ \frac{c}{bc-ad} & \frac{-a}{bc-ad} \end{pmatrix}$$

Temos que o denominador $bc - ad \neq 0$, pois estamos considerando matrizes inversíveis. Logo, $GL_2(\mathbb{R})$ é um grupo. Tome $A, B \in GL_2(\mathbb{R})$ onde

$$A = \begin{pmatrix} 1 & -3 \\ 7 & 2 \end{pmatrix}$$

e

$$B = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$$

Temos que

$$A \cdot B = \begin{pmatrix} 1 & -3 \\ 7 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -7 \\ 7 & -3 \end{pmatrix}$$

e, por outro lado,

$$B \cdot A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ 7 & 2 \end{pmatrix} = \begin{pmatrix} -6 & -5 \\ 14 & 4 \end{pmatrix}$$

Logo, $GL_2(\mathbb{R})$ é um grupo não abeliano.
De maneira geral, definimos os grupos lineares de grau n multiplicativos de matrizes inversíveis ($GL_n(K)$) onde K é um corpo.

Exemplo 2.9. Grupos de permutações S_n. Para exemplificar, utilizaremos um caso particular de S_n: o grupo de permutações S_3. O grupo S_3 é formado por elementos representados da seguinte maneira:

$$S_3 = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

onde a, b, c variam entre os números $1, 2$ e 3 sem repetições. A ideia desse conjunto é usar funções relacionando cada elemento da linha de cima com um elemento da linha de baixo. Desta forma, podemos interpretar um elemento genérico de S_3 da seguinte maneira:

$$f(1) = a$$
$$f(2) = b$$
$$f(3) = c$$

onde f é uma função bijetora de $\{1, 2, 3\}$ em $\{1, 2, 3\}$. Note que este grupo, com a operação de composição, tem seis elementos:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Vamos provar que S_3 é um grupo.
O primeiro elemento descrito acima representa a função identidade, logo,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

é o elemento neutro de S_3.
Agora, considere o elemento abaixo:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Vamos mostrar que ele é inverso de si mesmo.
Seja f_1 a função que representa este elemento. Usando a composição de funções, temos que:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ (f_1 \circ f_1)(1) & (f_1 \circ f_1)(2) & (f_1 \circ f_1)(3) \end{pmatrix}$$

Assim, fazendo a composição de f_1 com ela mesma, segue que

$$\begin{pmatrix} 1 & 2 & 3 \\ (f_1(f_1(1)) & (f_1(f_1(2)) & (f_1(f_1(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ f_1(2) & f_1(1) & f_1(3) \end{pmatrix}$$

resultando em

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Analogamente, podemos verificar que os seguintes elementos de S_3 também são inversos deles próprios:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Os dois elementos restantes são inversos um do outro:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

e consequentemente

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Portanto, as Propriedades 2 e 3 estão satisfeitas.
Como a composição de funções é associativa, segue que para quaisquer f_i, f_j e f_k, com i, j e k variando de 1 até 6, tem-se que

$$f_i \circ (f_j \circ f_k) = (f_i \circ f_j) \circ f_k$$

Portanto, S_3 é um grupo, e generalizando esse resultado pode-se provar que S_n é um grupo.

Definição 2.3. Sejam G um grupo e $g \in G$. A ordem de g é o menor inteiro positivo n tal que $g^n = 1$. Caso não exista tal n, dizemos que g tem ordem infinita.

Note que o elemento neutro é o único elemento dos grupos que tem ordem 1.

Exemplo 2.10. Uma operação binária em um conjunto finito pode ser apresentada através de uma tabela, por vezes chamada *tabela de Cayley*, tábua ou tabela de multiplicação. Desta forma, podemos utilizar este recurso para representar os elementos de um grupo e verificar as propriedades da operação de um modo sistemático. Construiremos a tabela do grupo dos quatérnios, representado por Q_8:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Tabela 1 – Tabela de multiplicação de Q_8

Analisando a tabela, podemos perceber que o elemento neutro deste grupo é o número 1, pois para qualquer $q \in Q_8$ temos que

$$1 \cdot q = q \cdot 1 = q$$

e ainda, que a operação é fechada, ou seja, operando quaisquer dois elementos de Q_8, o elemento resultante da operação pertence a Q_8. Também podemos observar que todos os elementos de Q_8 possuem inverso, configurando assim um grupo. Observe que

$$i \cdot j \neq j \cdot i$$

logo, este grupo não é abeliano. Por fim, note que -1 é o único elemento de Q_8 com ordem 2, os demais possuem ordem 4.

Exemplo 2.11. Seja D_4 o conjunto das simetrias de um quadrado. As transformações espaciais que preservam um quadrado são as rotações planas de $0, \frac{\pi}{2}, \pi$ e $\frac{3\pi}{2}$, no sentido anti-horário (chamaremos estas de r_0, r_1, r_2, r_3) e as rotações espaciais de π radianos com relação às diagonais e às mediatrizes do quadrado. Fixando uma diagonal, chamaremos de s a rotação de π radianos em torno de s, e compondo esta rotação com as rotações planas descritas anteriormente obtemos o restante das transformações espaciais que preservam o quadrado.

Representaremos as rotações espaciais por $s, r_1 \circ s, r_2 \circ s, r_3 \circ s$. Assim, com a composição de funções,

$$D_4 = \{r_0, r_1, r_2, r_3, s, r_1 \circ s, r_2 \circ s, r_3 \circ s\}$$

é um grupo não abeliano, pois

$$s \circ (s \circ r_1) = r_1$$

e

$$(s \circ r_1) \circ s = r_3$$

A tabela deste grupo pode ser consultada na página 79 de [3], onde pode-se notar que r_1 e r_3 têm ordem 4 e os cinco elementos restantes possuem ordem 2.

2.1 SUBGRUPOS

Quando sabemos que G é um grupo, podemos olhar para determinados subconjuntos de G que possuem características de grupo. Estes subconjuntos de G são chamados de subgrupos, como será formalizado na próxima definição.

Definição 2.4. Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G e denotamos por $H \leqslant G$, quando H é um grupo com a mesma operação de G.

Naturalmente, um grupo G é um subgrupo dele mesmo. Ainda, o elemento neutro de G também forma um subgrupo. Este grupo pode ser denotado por $\{1\}$ ou simplesmente por 1. Estes dois subgrupos de um grupo G qualquer são chamados de *subgrupos triviais*. É importante observar que, como H é subgrupo de G, os elementos de H acabam "herdando" características do próprio G, como discutiremos nas proposições seguintes.

Proposição 2.5. Sejam G um grupo e $H \leqslant G$. O elemento neutro de H é igual ao elemento neutro de G.

Demonstração. Dados 1_H e 1_G os respectivos elementos neutros de H e G, note que

$$1_H \cdot 1_H = 1_H$$

em H e

$$1_H \cdot 1_G = 1_H$$

em G. Multiplicando ambas equações à esquerda por 1_H^{-1}, concluímos que $1_H = 1_G$. □

Proposição 2.6. Sejam G um grupo e $H \leqslant G$. O inverso de um elemento em H é o mesmo que em G.

Demonstração. Seja $h \in H$. Temos que $h \cdot h^{-1} = h^{-1} \cdot h = 1_H$, em que h^{-1} é o inverso de h em $H \subseteq G$. Mas como $h \in G$, segue que existe um $g \in G$ tal que $g \cdot h = h \cdot g = 1_G$. Pela unicidade do inverso segue que $g = h^{-1}$. □

Proposição 2.7. Seja H um subgrupo de um grupo qualquer. Então

$$H^2 = HH = \{h_1 h_2 : h_1, h_2 \in H\} = H$$

Demonstração. Por definição, a operação entre quaisquer dois elementos de H está em H, logo, $H^2 \subseteq H$. Por outro lado, podemos escrever qualquer $h \in H$ como $h \cdot 1$, assim, $H \subseteq H^2$. □

Proposição 2.8. Seja H um subconjunto não-vazio de G. Assim, H é um subgrupo se, e somente se, as duas condições abaixo são satisfeitas.

1. $h_1 \cdot h_2 \in H,\ \forall\, h_1, h_2 \in H$
2. $h^{-1} \in H,\ \forall\, h \in H$

Demonstração. Suponha que $H \leqslant G$. Logo, por definição, H é um grupo e consequentemente, as duas condições são satisfeitas.
Por outro lado, suponha que H seja um subconjunto não vazio de G. Como G é um grupo, todos os seus elementos satisfazem a associatividade, em particular, todos os elementos de H.
Por hipótese, $h_1 \cdot h_2 \in H,\ \forall\ h_1, h_2 \in H$, logo, H é fechado para a operação. Ainda temos, pela hipótese (2), que

$$h^{-1} \in H,\ \forall\ h \in H$$

então, pela hipótese (1)

$$h \cdot h^{-1} \in H$$

e consequentemente, existe $1_H \in H$. Como provamos que o inverso e o elemento neutro são únicos, segue que $H \leqslant G$. □

Esta proposição é importante pois a verificação de que um subconjunto é subgrupo se torna mais simples. Vamos ver alguns exemplos de subgrupos, e demonstrar que de fato são subgrupos usando a Proposição 2.8.

Exemplo 2.12. O conjunto dos múltiplos de determinado $n \in \mathbb{Z}$, denotado por $n\mathbb{Z}$, é um subgrupo de $(\mathbb{Z}, +)$. Pela Proposição 2.8, visto que $n\mathbb{Z}$ é claramente não-vazio, precisamos mostrar que $n\mathbb{Z}$ satisfaz duas propriedades. Note que um elemento deste grupo é do tipo nz, onde n é fixo e z um número inteiro qualquer. Lembrando que a operação do grupo $\mathbb{Z}$ é a adição usual.
Considere $x, y \in \mathbb{Z}$. Temos que

$$nx + ny = n(x + y)$$

$$\implies n(x + y) \in n\mathbb{Z}$$

Logo, ao operarmos dois elementos quaisquer em $n\mathbb{Z}$ o elemento resultante ainda é da forma nz.
Sendo $nz \in n\mathbb{Z}$, o seu inverso será $n(-z)$, pois

$$nz + n(-z) = nz + (-nz) = nz - nz = n(z - z) = 0$$

Portanto, $n\mathbb{Z} \leqslant \mathbb{Z}$.

Exemplo 2.13. Os elementos de um grupo G que comutam com qualquer elemento do grupo formam um subconjunto de G. Este subconjunto é denominado Centro de G e definido por

$$\mathcal{Z}(G) = \{x \in G : xg = gx \quad \forall\, g \in G\}$$

Qualquer grupo terá pelo menos um elemento no centro, o elemento neutro. Vamos mostrar que $\mathcal{Z}(G)$ é um subgrupo de G.
Se $x_1, x_2 \in \mathcal{Z}(G)$, então, $x_1 g = g x_1$ e $x_2 g = g x_2$, $\forall\, g \in G$. Assim,

$$x_1 x_2 g = x_1 g x_2 = g x_1 x_2$$

Portanto, $x_1 x_2 \in \mathcal{Z}(G)$.
Seja $x \in \mathcal{Z}(G)$. Vamos verificar se $x^{-1} \in \mathcal{Z}(G)$:

$$x^{-1} g = x^{-1} g x x^{-1} = x^{-1} x g x^{-1} = g x^{-1}$$

Logo, $\mathcal{Z}(G) \leqslant G$.

Observação 2.2. *Dado um grupo G, temos que $\mathcal{Z}(G) = G$ se, e somente se, G é abeliano.*

Proposição 2.9. Se H e K são subgrupos de G então $H \cap K$ é um subgrupo de G.

Demonstração. Note que $H \cap K$ é não-vazio, pois contém 1. Sejam $a, b \in H \cap K$. Temos então que $a, b \in H$ e $a, b \in K$. Como cada

um destes é um subgrupo de G, segue que $ab \in H$ e $ab \in K$. Logo, $ab \in H \cap K$.
Seja $a \in H \cap K$. Portanto, a pertence a cada um destes dois subgrupos de G, o que significa que $a^{-1} \in H$ e $a^{-1} \in K$. Assim, $a^{-1} \in H \cap K$. Portanto, $H \cap K$ é um subgrupo de G. □

Exemplo 2.14. Sejam $\mathbb{Z}_6$ e $H = \{\overline{0}, \overline{3}\}$ um subconjunto de $\mathbb{Z}_6$. Mostraremos que H é um subgrupo. Como H tem apenas dois elementos, podemos mostrar que H é um subgrupo verificando se seus elementos obedecem as regras para H ser um subgrupo sem a necessidade de usar elementos genéricos.
Note que

$$\begin{aligned} \overline{0} + \overline{3} = \overline{3} + \overline{0} = \overline{3} \in H \\ \overline{0} + \overline{0} = \overline{0} \in H \\ \overline{3} + \overline{3} = \overline{6} = \overline{3} \in H \end{aligned}$$

Portanto, H é fechado para a operação $+$.
Ainda, $\overline{0}^{-1} = \overline{0} \in H$ e $\overline{3}^{-1} = \overline{3} \in H$. Desta forma, $H = \{\overline{0}, \overline{3}\}$ é um subgrupo de $\mathbb{Z}_6$.

Exemplo 2.15. Vimos no Exemplo 2.8 o grupo $GL_2(\mathbb{R})$. Considere o subconjunto $SL_2(\mathbb{R})$ como sendo o grupo das matrizes 2×2 com determinante igual a 1. Este subconjunto é um subgrupo de $GL_2(\mathbb{R})$. Sendo $A, B \in SL_2(\mathbb{R})$, segue que

$$det(AB) = det(A)det(B) = 1 \cdot 1 = 1$$

e como

$$det(A^{-1}) = det(A)^{-1} = \frac{1}{det(A)} = \frac{1}{1} = 1$$

o subgrupo é fechado para a operação e para cada $A \in SL_2(\mathbb{R})$, $A^{-1} \in SL_2(\mathbb{R})$. Portanto, $SL_2(\mathbb{R}) \leqslant GL_2(\mathbb{R})$.

Sabemos que uma relação de equivalência é uma relação binária que satisfaz três propriedades: as propriedades reflexiva, simétrica e transitiva. A partir deste conceito, vamos construir a ideia de relações de equivalência usando um grupo e seus subgrupos. Na próxima definição, a relação será explicitada. Usaremos a seguinte notação: $y \sim_E x$ (lê-se "y se relaciona com x" ou "y é equivalente à x").

Definição 2.5. Sejam G um grupo e $H \leqslant G$. Considere a seguinte relação de equivalência em G:

$$x, y \in G,\ y \sim_E x \iff \exists\, h \in H :\ y = xh$$

A classe de equivalência

$$\{y \in G : y\ \sim_E\ x\} = \{xh :\ h \in H\} = xH$$

é chamada de classe lateral de x à esquerda, e note que

$$y \in xH \iff yH = xH$$

De maneira análoga, pode-se definir a classe lateral de x à direita:

$$\{hx : h \in H\} = Hx$$

Observação 2.3. *Se G for um grupo aditivo, representaremos a classe lateral por $x + H$ ou $H + x$.*

2.2 SUBGRUPOS NORMAIS E GRUPO QUOCIENTE

Uma vez que sabemos o que são subgrupos, podemos categorizá-los de acordo com suas características. Quando um subgrupo é preservado por uma conjugação, ele recebe o nome de subgrupo normal. Desta forma, pode-se definir o grupo quociente usando o conceito de classes laterais, como veremos nas próximas páginas.

Definição 2.6. Sejam G um grupo e $N \leqslant G$. N é um subgrupo normal de G (denota-se $N \trianglelefteq G$) se N satisfaz uma das seguintes afirmações equivalentes:

1. $gNg^{-1} \subseteq N,\ \forall\ g \in G$

2. $gNg^{-1} = N,\ \forall\ g \in G$

3. $gN = Ng,\ \forall\ g \in G$

Para mostrar que determinado $N \subseteq G$ é um subgrupo normal, primeiramente deveremos mostrar que N é um subgrupo de G, e em seguida provar uma das afirmações da Definição 2.6. Vamos ver alguns exemplos de subgrupos normais nas próximas páginas.

Exemplo 2.16. Dado um grupo G, 1 e G são subgrupos normais triviais de G. Já sabemos que 1 e G são subgrupos de G. Veja que 1 é um subgrupo normal de G, pois $1H = H1$. O grupo G é um subconjunto normal dele mesmo pois $gGg^{-1} \subseteq G\ \forall\ g \in G$.

Exemplo 2.17. Considere o subgrupo $\mathcal{Z}(G)$ apresentado no Exemplo 2.13. Se $H \subseteq \mathcal{Z}(G)$ então $H \trianglelefteq G$.
Para provar que $H \trianglelefteq G$, precisamos mostrar que uma das condições da Definição 2.6 é satisfeita pelos elementos deste grupo.
Seja $h \in H$ e $g \in G$. Precisamos mostrar que $ghg^{-1} \in H$. Se $h \in H$, pelo fato de que $H \subseteq \mathcal{Z}(G)$ então $h \in \mathcal{Z}(G)$ e assim,

$$ghg^{-1} = hgg^{-1} = h$$

Em particular, $ghg^{-1} \in H$ e portanto $H \trianglelefteq G$.

Observação 2.4. *Se G é abeliano, todos os subgrupos de G são normais.*

Definição 2.7. Sejam G um grupo e $H \trianglelefteq G$. Então o conjunto das classes laterais, com a operação

$$gH \cdot kH = gkH$$

é o grupo quociente de G por H, denotado por G/H.

Exemplo 2.18. Sejam $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e $H = \{\overline{0}, \overline{3}\}$. Como demonstrado no Exemplo 2.14, H é um subgrupo de $\mathbb{Z}_6$ e como $\mathbb{Z}_6$ é abeliano, H é um subgrupo normal.
As classes laterais são:

$$\overline{0} + H = H$$
$$\overline{1} + H = \{\overline{1}, \overline{4}\}$$
$$\overline{2} + H = \{\overline{2}, \overline{5}\}$$

Abaixo, temos a tabela do grupo quociente $\mathbb{Z}_6/H$:

$+$	H	$\overline{1}+H$	$\overline{2}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	H
$\overline{2}+H$	$\overline{2}+H$	H	$\overline{1}+H$

Tabela 2 – Grupo quociente $\mathbb{Z}_6/H$

2.3 HOMOMORFISMOS

A partir deste ponto do trabalho, vamos trabalhar com aplicações entre dois grupos. Quando uma aplicação entre dois grupos preserva a estrutura dos mesmos, ela recebe o nome de homomorfismo. Esta aplicação ainda pode ser injetora, sobrejetora ou bijetora. Vamos formalizar esta ideia na próxima definição.

Definição 2.8. Sejam $(G, \cdot)$ e $(H, *)$ grupos. Uma função

$$\varphi : G \to H$$

é um homomorfismo de grupos se

$$\varphi(g \cdot h) = \varphi(g) * \varphi(h),\ \forall\ g, h \in G$$

Exemplo 2.19. A aplicação $Id : G \to G,\ Id(g) = g$ é um homomorfismo chamado identidade. Vamos mostrar que Id é um homomorfismo. Sejam $g, h \in G$. Temos que

$$Id(gh) = gh = Id(g)Id(h)$$

Logo, a função identidade é um homomorfismo.

Exemplo 2.20. Sejam G, H grupos e α uma função.

$$\begin{aligned} \alpha : G &\to H \\ g &\mapsto 1_H \end{aligned}$$

é um homomorfismo chamado homomorfismo trivial. De fato, sendo $g_1, g_2 \in G$, segue que

$$\alpha(g_1 g_2) = 1_H = 1_H 1_H = \alpha(g_1)\alpha(g_2)$$

Exemplo 2.21. Sejam $m, n \in \mathbb{Z}$, e $\varphi_m : (\mathbb{Z}_n, +) \to (\mathbb{Z}_n, +)$ onde $\varphi_m(\overline{z}) = \overline{mz}$. Esta aplicação é um homomorfismo, pois, sendo $\overline{z_1}, \overline{z_2} \in \mathbb{Z}_n$,

$$\begin{aligned} \varphi_m(\overline{z_1} + \overline{z_2}) &= \varphi_m(\overline{z_1 + z_2}) \\ &= \overline{m(z_1 + z_2)} \\ &= \overline{mz_1 + mz_2} \\ &= \overline{mz_1} + \overline{mz_2} \\ &= \varphi_m(\overline{z_1}) + \varphi_m(\overline{z_2}) \end{aligned}$$

Exemplo 2.22. Se G é abeliano, então

$$\begin{aligned} \alpha_n : G &\to G \\ g &\mapsto g^n \end{aligned}$$

é um homomorfismo. De fato:

$$\alpha_n(g_1g_2) = (g_1g_2)^n = {g_1}^n{g_2}^n = \alpha_n(g_1)\alpha_n(g_2)$$

Exemplo 2.23. Seja G um grupo e $N \trianglelefteq G$. Então

$$\varphi : G \to G/N$$
$$g \mapsto gN$$

é um homomorfismo, pois

$$\begin{aligned} \varphi(g_1g_2) &= g_1g_2N \\ &= g_1Ng_2N \\ &= \varphi(g_1)\varphi(g_2) \end{aligned}$$

Este homomorfismo recebe o nome de projeção canônica.

Vinculado ao homomorfismo de grupo, a seguir veremos dois conceitos importantes: o núcleo e a imagem de um homomorfismo.

Definição 2.9. Seja $\varphi : G \to H$ um homomorfismo de grupos. Se 1_H indica o elemento neutro de H, o núcleo de φ é o seguinte subconjunto:

$$Ker(\varphi) = \{g \in G : \varphi(g) = 1_H\}$$

Observação 2.5. *A notação da Definição 2.9 vem do inglês, da tradução de núcleo (kernel).*

Definição 2.10. Seja $\varphi : G \to H$ um homomorfismo de grupos. O seguinte subconjunto de H

$$Im(\varphi) = \{h \in H : h = \varphi(g) \text{ para algum } g \in G\}$$

é denominado imagem de φ.

A seguir, observaremos algumas proposições importantes de homomorfismos.

Proposição 2.10. Seja $\varphi : (G, \cdot) \to (H, *)$ um homomorfismo de grupos. Então $\varphi(1_G) = 1_H$.

Demonstração. De fato, $\forall\, g \in G$, temos que

$$\begin{aligned} \varphi(1_G) &= \varphi(1_G \cdot 1_G) \\ \implies \varphi(1_G) &= \varphi(1_G) * \varphi(1_G) \\ \implies (\varphi(1_G))^{-1} * \varphi(1_G) &= (\varphi(1_G))^{-1} * \varphi(1_G) * \varphi(1_G) \\ \implies 1_H &= \varphi(1_G) \end{aligned}$$

□

Proposição 2.11. Seja $\varphi : (G, \cdot) \to (H, *)$ um homomorfismo de grupos. Então $\varphi(g)^{-1} = \varphi(g^{-1})$.

Demonstração. Temos que

$$\begin{aligned} 1_H &= \varphi(1_G) \\ &= \varphi(g \cdot g^{-1}) \\ &= \varphi(g) * \varphi(g^{-1}) \\ \implies \varphi(g)^{-1} &= \varphi(g^{-1}) \end{aligned}$$

□

Proposição 2.12. Seja φ um homomorfismo de grupos. Desta forma, $Ker(\varphi) = \{1\}$ se, e somente se, φ é injetora.

Demonstração. Suponha que $Ker(\varphi) = \{1\}$. Vamos mostrar que φ é uma aplicação injetora.

Seja $\varphi(a) = \varphi(b)$, queremos provar que $a = b$.

$$\begin{aligned} \varphi(a) &= \varphi(b) \\ \Rightarrow \varphi(a) \cdot \varphi(b)^{-1} &= \varphi(b) \cdot \varphi(b)^{-1} \\ \Rightarrow \varphi(a) \cdot \varphi(b)^{-1} &= 1 \\ \Rightarrow \varphi(ab^{-1}) &= 1 \end{aligned}$$

Desta forma, $ab^{-1} \in Ker(\varphi)$, e por hipótese:

$$\begin{aligned} ab^{-1} &= 1 \\ \Rightarrow a &= b \end{aligned}$$

Portanto, φ é injetora.
Por outro lado, suponha que φ seja injetora. Seja $g \in Ker(\varphi)$.

$$\begin{aligned} \varphi(g) &= 1 \\ \Longrightarrow \varphi(g) &= \varphi(1) \\ \Longrightarrow g &= 1 \end{aligned}$$

Assim, $Ker(\varphi) = \{1\}$. □

Proposição 2.13. Seja $\varphi : G \to H$ um homomorfismo de grupos. O núcleo de φ é um subgrupo normal de G.

Demonstração. Sejam $g_1, g_2 \in Ker(\varphi)$. Então

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 1_H 1_H = 1_H$$

e

$$\varphi(g^{-1}) = \varphi(g)^{-1} = 1_H^{-1} = 1_H$$

Portanto, $Ker(\varphi)$ é um subgrupo de G. Agora, precisamos provar que $Ker(\varphi)$ é um subgrupo normal de G.

Dado $x \in Ker(\varphi)$, vamos mostrar que $\varphi(gxg^{-1}) = 1_H$. De fato:

$$\begin{aligned} \varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g^{-1}) \\ &= \varphi(g)1_H\varphi(g^{-1}) \\ &= \varphi(g)\varphi(g^{-1}) \\ &= \varphi(gg^{-1}) \\ &= 1_H \end{aligned}$$

□

Se um homomorfismo é uma aplicação injetora, então é chamado de homomorfismo injetor. Da mesma forma, se um homomorfismo é uma aplicação sobrejetora é chamado de homomorfismo sobrejetor. O caso em que o homomorfismo é bijetor corresponde ao conceito de isomorfismo e será apresentado adiante.

Exemplo 2.24. Considere os elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\alpha_1 = (\bar{1}, \bar{0})$, $\alpha_2 = (\bar{0}, \bar{1})$, $\alpha_3 = (\bar{1}, \bar{1})$. Então, variando i de 1 a 3, definimos três funções

$$\begin{aligned} f_i : \mathbb{Z}_2 &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \bar{0} &\mapsto (\bar{0}, \bar{0}) \\ \bar{1} &\mapsto \alpha_i \end{aligned}$$

Todas essas três funções são homomorfismos injetivos.

Exemplo 2.25. Seja $a \in \mathbb{Z}$. A aplicação

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z} \\ m &\mapsto am \end{aligned}$$

é um homomorfismo, pois

$$\begin{aligned} f(m+n) &= a(m+n) \\ &= am+an \\ &= f(m)+f(n) \end{aligned}$$

Quando $a \neq 0$, f é injetora:

$$\begin{aligned} f(m) &= f(n) \\ am &= an \\ \Rightarrow m &= n \end{aligned}$$

Quando $a = 1$, f também é sobrejetora.

A seguir, observe alguns exemplos de homomorfismos sobrejetores.

Exemplo 2.26. A aplicação

$$\begin{aligned} f : \mathbb{C}^* &\to \mathbb{R}_+^* \\ z &\mapsto |z| \end{aligned}$$

é um homomorfismo sobrejetor.
Vamos provar que f é um homomorfismo:

$$f(zw) = |zw| = |z||w| = f(z)f(w)$$

Agora, falta mostrar que f é sobrejetora. De fato, seja $a \in \mathbb{R}_+^*$, então $a + 0i$ tem a imagem igual à a pela aplicação f, pois $f(a) = |a| = a$.

Exemplo 2.27. Considere $n > 1$ e $f_n : \mathbb{Z} \to \mathbb{Z}_n$, definida por $f_n(a) = \overline{a}$. Então, f_n é um homomorfismo sobrejetor pois

$$f_n(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f_n(a) + f_n(b)$$

e, dado $\overline{a} \in \mathbb{Z}_n$, temos que $f_n(a) = \overline{a}$. Portanto, f_n é um homomorfismo sobrejetor.

Definição 2.11. Seja $f : G \to H$ um homomorfismo de grupos. Se f for uma aplicação bijetora, dizemos que f é um isomorfismo do grupo G no grupo H, e que G é isomorfo a H. Denotamos por $G \simeq H$.

Vejamos alguns exemplos de isomorfismos de grupos.

Exemplo 2.28. Seja G um grupo e $g \in G$. Então

$$\begin{aligned} \phi : G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

é um isomorfismo de grupos.
De fato, note que

$$\phi(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \phi(x_1)\phi(x_2)$$

Portanto, ϕ é um homomorfismo. Agora, falta provar que ϕ é bijetora. Sejam $x_1, x_2 \in G$. Suponha $\phi(x_1) = \phi(x_2)$

$$\begin{aligned} \phi(x_1) &= \phi(x_2) \\ \Rightarrow gx_1g^{-1} &= gx_2g^{-1} \\ \Rightarrow x_1 &= x_2 \end{aligned}$$

Logo, ϕ é injetora. Ela é sobrejetora pois, dado $h \in G$, temos que $\phi(g^{-1}hg) = h$.

Exemplo 2.29. Considere os grupos G e H grupos e o produto direto $G \times H$. Temos que $G \times \{1\}$ e $\{1\} \times H$ são subgrupos de $G \times H$ e que $G \times \{1\}$ é isomorfo à G.
Considere a função $\varphi : G \to G \times \{1\}$ definida por $\varphi(g) = (g, 1)$. Sendo $g_1, g_2 \in G$, φ é um homomorfismo:

$$\varphi(g_1g_2) = (g_1g_2, 1) = (g_1, 1)(g_2, 1) = \varphi(g_1)\varphi(g_2)$$

Temos que φ é injetora, pois

$$\begin{aligned} \varphi(g_1) &= \varphi(g_2) \\ \implies (g_1, 1) &= (g_2, 1) \\ \implies g_1 &= g_2 \end{aligned}$$

Agora, dado $(g, 1) \in G \times \{1\}$, como $\varphi(g) = (g, 1)$, segue que φ é sobrejetora. Portanto, φ é um isomorfismo e G é isomorfo à $G \times \{1\}$. Analogamente, H é isomorfo a $\{1\} \times H$.

Exemplo 2.30. Os grupos $\{\pm 1\}$ (com a operação usual de produto) e $\mathbb{Z}_2$ são isomorfos, pois podemos definir

$$\begin{aligned} \phi : \{\pm 1\} &\to \mathbb{Z}_2 \\ 1 &\mapsto \overline{0} \\ -1 &\mapsto \overline{1} \end{aligned}$$

onde ϕ é um homomorfismo bijetor.

Se $\varphi : G \to H$ é um isomorfismo, φ é bijetora e naturalmente podemos esperar que exista $\varphi^{-1} : H \to G$.

Proposição 2.14. Se $\varphi : G \to H$ é um isomorfismo, então $\varphi^{-1} : H \to G$ também é um isomorfismo.

Demonstração. Como φ é bijetora, sabemos que existe φ^{-1} também bijetora. Precisamos mostrar que φ^{-1} é um homomorfismo.
Tome $h_1, h_2 \in H$. Como φ é sobrejetora, existem $g_1, g_2 \in G$ tais que $\varphi(g_1) = h_1$ e $\varphi(g_2) = h_2$.
Então

$$\varphi^{-1}(h_1) = \varphi^{-1}\varphi(g_1) = g_1$$

e analogamente $\varphi^{-1}(h_2) = g_2$. Assim:

$$\begin{aligned} \varphi^{-1}(h_1h_2) &= \varphi^{-1}(\varphi(g_1)\varphi(g_2)) \\ &= \varphi^{-1}(\varphi(g_1g_2)) \\ &= g_1g_2 \\ &= \varphi^{-1}(h_1)\varphi^{-1}(h_2) \end{aligned}$$

Desta forma, φ^{-1} é um isomorfismo. □

A partir da existência de um homomorfismo $\beta : G \to H$, é possível utilizar o núcleo do mesmo para obter um isomorfismo entre o grupo quociente $G/Ker(\beta)$ e o a imagem de β. O próximo teorema, denominado *Teorema do isomorfismo*, exibirá quem é este isomorfismo e a maneira que ele é definido.

Teorema 2.1. *(Teorema do isomorfismo) Seja $\beta : G \to H$ um homomorfismo de grupos. A função induzida*

$$\begin{aligned} \overline{\beta} : G/Ker(\beta) &\to Im(\beta) \\ gKer(\beta) &\mapsto \beta(g) \end{aligned}$$

é um isomorfismo.

Demonstração. Inicialmente é preciso verificar se $\overline{\beta}$ está bem definida, ou seja, que

$$gKer(\beta) = \overline{g}Ker(\beta) \implies \beta(g) = \beta(\overline{g})$$

De fato:

$$gKer(\beta) = \overline{g}Ker(\beta) \implies g \in \overline{g}Ker(\beta)$$

Logo, $g = \overline{g}k$ com $k \in Ker(\beta)$.
Assim,

$$\beta(g) = \beta(\overline{g}k) = \beta(\overline{g})\beta(k) = \beta(\overline{g})$$

Logo, $\overline{\beta}$ está bem definida. Ainda, temos que

$$\begin{aligned}\overline{\beta}(gKer(\beta)\cdot\overline{g}Ker(\beta)) &= \overline{\beta}(g\overline{g}Ker(\beta))\\ &= \beta(g\overline{g})\\ &= \beta(g)*\beta(\overline{g})\\ &= \overline{\beta}(gKer(\beta))*\overline{\beta}(\overline{g}Ker(\beta))\end{aligned}$$

Desta forma, $\overline{\beta}$ é um homomorfismo.
Agora, vamos provar que $\overline{\beta}$ é sobrejetora. Seja $\beta(g)\in Im(\beta)$. Temos que $\beta(g)=\overline{\beta}(gKer(\beta))$.
Resta mostrar que $\overline{\beta}$ é injetora. Sejam $x,y\in G/Ker(\beta)$, tais que $\overline{\beta}(xKer(\beta))=\overline{\beta}(yKer(\beta))$.Vamos mostrar que $xKer(\beta)=yKer(\beta)$.

$$\begin{aligned}\overline{\beta}(xKer(\beta)) &= \overline{\beta}(yKer(\beta))\\ \Longrightarrow\ \beta(x) &= \beta(y)\\ \Longrightarrow\ \beta(x)\beta(y)^{-1} &= 1\\ \Longrightarrow\ \beta(x)\beta(y^{-1}) &= 1\\ \Longrightarrow\ \beta(xy^{-1}) &= 1\end{aligned}$$

Assim, $xy^{-1}\in Ker(\beta)$, e $xKer(\beta)=yKer(\beta)$. Logo, $\overline{\beta}$ é injetora, e segue o resultado. □

Nos próximos exemplos veremos algumas aplicações do Teorema 2.1.

Exemplo 2.31. Considere o homomorfismo apresentado no Exemplo 2.27. Temos que $f_n:\mathbb{Z}\to\mathbb{Z}_n$ definida por $f_n(a)=\overline{a}$ é um homomorfismo sobrejetor e assim, $Im(f_n)=\mathbb{Z}_n$. Vejamos quais são os elementos que estão no núcleo de f_n.
Tome $a\in Ker(f_n)$, logo

$$f_n(a)=\overline{0}$$

e portanto a deverá ser um múltiplo de n. Logo, $Ker(f_n) = n\mathbb{Z}$ e pelo Teorema 2.1, segue que

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$$

Exemplo 2.32. Seja $\beta : D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ um homomorfismo, onde D_4 é o grupo das simetrias do quadrado apresentado no Exemplo 2.11. O homomorfismo β é definido da seguinte maneira:

$$r_1 \mapsto (\overline{1}, \overline{0})$$
$$s \mapsto (\overline{0}, \overline{1})$$

Podemos estender β homomorficamente para os outros elementos de D_4, ou seja, como os demais elementos de D_4 podem ser obtidos a partir de r_1 e s, definir β neste dois elementos é suficiente.
Analisando as imagens dos elementos de D_4 é possível perceber que

$$Ker(\beta) = \{r_0, r_2\}$$

e

$$Im(\beta) = \mathbb{Z}_2 \times \mathbb{Z}_2$$

Pelo Teorema 2.1, existe um isomorfismo

$$\overline{\beta} : D_4/Ker(\beta) \to \mathbb{Z}_2 \times \mathbb{Z}_2$$

ou seja,

$$D_4/\{r_0, r_2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

Exemplo 2.33. Seja $\beta : Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ definido por:

$$\pm 1 \mapsto (\overline{0}, \overline{0})$$
$$\pm i \mapsto (\overline{1}, \overline{0})$$
$$\pm j \mapsto (\overline{0}, \overline{1})$$
$$\pm k \mapsto (\overline{1}, \overline{1})$$

Temos que β é um homomorfismo, que $Ker(\beta) = \{\pm 1\}$ e

$$Im(\beta) = \mathbb{Z}_2 \times \mathbb{Z}_2$$

Pelo Teorema do isomorfismo, $Q_8/\{\pm 1\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Podemos deduzir a partir dos Exemplos 2.32 e 2.33, que o grupo $D_4/\{r_0, r_2\}$ é isomorfo ao grupo $Q_8/\{\pm 1\}$.

Teorema 2.2. *Sejam G e H dois grupos isomorfos. Então para qualquer n inteiro positivo, G e H têm o mesmo número de elementos de ordem n.*

A demonstração do Teorema 2.2 pode ser consultada na página 77 da referência [6].

Definição 2.12. Seja G um grupo. Um automorfismo de G é um isomorfismo

$$\phi : G \to G$$

O conjunto dos automorfismos de G será denotado por $Aut(G)$.

O conjunto dos automorfismos de um grupo G é um grupo com a operação de composição de funções. Como se tratam de isomorfismos, pela Proposição 2.14, cada elemento de $Aut(G)$ tem um inverso que também está em $Aut(G)$. Além disso, a composição de funções é associativa, e ainda, a função identidade é um isomorfismo que neste caso será o elemento neutro.

O Exemplo 2.28 nos mostra um isomorfismo de um grupo nele mesmo, portanto um automorfismo, chamado de *automorfismo interno*.

Exemplo 2.34. Sejam H e K grupos. Considere o grupo dos automorfismos de H. A função

$$\phi : K \to Aut(H)$$
$$k \mapsto \phi_k$$

é um homomorfismo, e $\phi(k)(h) = \phi_k(h) = khk^{-1} \in Aut(H)$ para qualquer $k \in K$.
Inicialmente mostraremos que ϕ é um homomorfismo. Tome $k_1, k_2 \in K$ e $h \in H$. Temos que

$$\begin{aligned} \phi_{k_1}\phi_{k_2}(h) &= \phi_{k_1}(k_2 h k_2^{-1}) \\ &= k_1 k_2 h k_2^{-1} k_1^{-1} \\ &= k_1 k_2 h (k_1 k_2)^{-1} \\ &= \phi_{k_1 k_1}(h) \end{aligned}$$

Logo, ϕ é um homomorfismo.
Vamos mostrar que $\phi_k \in Aut(H)$. Sejam $h_1, h_2 \in H$. Assim,

$$\begin{aligned} \phi_k(h_1 h_2) &= k h_1 h_2 k^{-1} \\ &= k h_1 k k^{-1} h_2 k^{-1} \\ &= \phi_k(h_1)\phi_k(h_2) \end{aligned}$$

Portanto, ϕ_k é um homomorfismo. Ainda, para qualquer $h \in H$ temos que $\varphi_k(k^{-1}hk) = kk^{-1}hkk^{-1} = h$, logo, ϕ_k é sobrejetora. Resta mostrar que ϕ_k é injetora. Suponha que $h \in Ker(\phi_k)$. Desta forma,

$$\begin{aligned} \phi_k(h) &= 1 \\ \implies khk^{-1} &= 1 \\ \implies kh &= k \\ \implies h &= k^{-1}k \\ \implies h &= 1 \end{aligned}$$

Portanto, ϕ_k é injetora e segue o resultado.

2.4 PRODUTO SEMIDIRETO

Vimos no Exemplo 2.6 uma maneira de obter um grupo a partir de dois grupos quaisquer usando o produto direto. Nesta seção,

veremos que existem outras ferramentas que nos permitem "criar" um novo grupo a partir de dois existentes. Para isso, estudaremos uma generalização do produto direto, denominado *produto semidireto*.

Considerando os grupos H e K, vamos tentar definir um novo grupo HK a partir deles. Intuitivamente, poderíamos pensar que este novo grupo seria algo do tipo:

$$HK = \{hk : h \in H, k \in K\}$$

A partir desta ideia inicial alguns questionamentos podem surgir. O que seria hk? Os grupos H e K poderiam ter naturezas completamente distintas, dificultando ou impossibilitando a operação entre os seus elementos. Outra questão seria como definir o produto entre dois elementos de HK. Precisamos garantir que o produto continue sendo do tipo hk.

A princípio, podemos impôr restrições para termos um conceito bem definido, por exemplo exigir que H e K sejam subgrupos do mesmo grupo G. Desta forma, hk será o resultado da operação de h e k dentro de G, e a operação de HK pode ser a operação "herdada" do grupo G. Um outro obstáculo é que precisamos que o elemento resultante desta operação seja um elemento de HK, ou seja, a operação

$$(h_1k_1)(h_2k_2) \tag{1}$$

precisa resultar em um elemento do tipo

$$h_3k_3$$

Visualmente falando, poderíamos trocar h_2 e k_1 de posição em (1). Poderíamos pensar em pedir que G fosse abeliano, mas assim perderíamos com esta restrição. Logo, uma alternativa viável é exigir que H seja normal em G. Lembrando que, de acordo com a Definição 2.6,

H é normal em G se

$$\forall h \in H, \forall k \in G, khk^{-1} \in H$$

Portanto, é possível fazer a seguinte manipulação entre os elementos:

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1k_1h_2(k_1^{-1}k_1)k_2 \\ &= h_1(k_1h_2k_1^{-1})k_1k_2\end{aligned}$$

Logo temos o resultado do tipo h_3k_3, onde $h_3 = h_1(k_1h_2k_1^{-1})$ e $k_3 = k_1k_2$, garantindo que este elemento pertença à HK. Assim é possível definir este grupo HK, que é um subgrupo de G. Perceba que o que foi feito foi considerar a função

$$\phi : K \to Aut(H)$$

dada por $\phi(k)(h) = khk^{-1}$. Mostramos no Exemplo 2.34 que ϕ é um homomorfismo e que, de fato $\phi(k)$ é um automorfismo de H, para qualquer $k \in K$. Vamos denotar $\phi(k)$ por ϕ_k.

Generalizando a construção acima, considere H e K dois grupos quaisquer, e φ um homomorfismo qualquer

$$\varphi : K \to Aut(H)$$

Agora, considere o produto cartesiano

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

com a operação:

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$$

Provaremos que esta estrutura é um grupo, e denotaremos o produto cartesiano munido da operação acima por $\rtimes_\varphi$.

Sejam $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \rtimes_\varphi K$. A operação deste grupo é associativa, pois

$$\begin{aligned}
[(h_1, k_1)(h_2, k_2)](h_3, k_3) &= (h_1\varphi_{k_1}(h_2), k_1k_2)(h_3, k_3) \\
&= (h_1\varphi_{k_1}(h_2)\varphi_{k_1k_2}(h_3), (k_1k_2)k_3) \\
&= (h_1\varphi_{k_1}(h_2\varphi_{k_2}(h_3)), k_1(k_2k_3)) \\
&= (h_1, k_1)(h_2\varphi_{k_2}(h_3), k_2k_3) \\
&= (h_1, k_1)[(h_2, k_2)(h_3, k_3)]
\end{aligned}$$

Observe que

$$\begin{aligned}
(h, k)(1_H, 1_K) &= (h\varphi_k(1_H), k1_K) \\
&= (h, k) \\
&= (1_Hh, k) \\
&= (1_H\varphi_{1_K}(h), 1_Kk) \\
&= (1_H, 1_K)(h, k)
\end{aligned}$$

Portanto, $(1_H, 1_K)$ é o elemento neutro. Vamos determinar o inverso de um elemento $(h.k) \in H \rtimes_\varphi K$. Temos que

$$\begin{aligned}
(h, k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) &= (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) \\
&= (h\varphi_{1_K}(h^{-1}), 1_K) \\
&= (hh^{-1}, 1_K) \\
&= (1_H, 1_K)
\end{aligned}$$

e por outro lado,

$$\begin{aligned}
(\varphi_{k^{-1}}(h^{-1}), k^{-1})(h, k) &= (\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), kk^{-1}) \\
&= (\varphi_{k^{-1}}(h^{-1}h), 1_K) \\
&= (\varphi_{k^{-1}}(1_H), 1_K) \\
&= (1_H, 1_K)
\end{aligned}$$

Portanto, $(h,k)^{-1} = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$. Logo, $H \rtimes_\varphi K$ é um grupo.

Definição 2.13. Sejam H, K grupos e $\varphi : K \to Aut(H)$ um homomorfismo. O grupo $H \rtimes_\varphi K$ é chamado de produto semidireto de H e K. Este grupo é o cartesiano de H e K munido da seguinte operação:

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2)$$

Vamos elucidar este conceito nos próximos exemplos.

Exemplo 2.35. Sejam $\mathbb{Z}_{2n}$ e H grupos, onde H é um grupo abeliano qualquer. Considere o homomorfismo

$$\varphi : \mathbb{Z}_{2n} \to Aut(H)$$

onde $\varphi_{\overline{k}}$ é uma função de H em H que leva um elemento no seu inverso se k é ímpar, e $\varphi_{\overline{k}}$ é a identidade se k é par.
Dado um $\overline{k} \in \mathbb{Z}_{2n}$, vamos provar que $\varphi_{\overline{k}} \in Aut(H)$ para todo $\overline{k}$. Para isso, precisamos mostrar que $\varphi_{\overline{k}}$ é um homomorfismo bijetor.
Iniciaremos mostrando que $\varphi_{\overline{k}}$ é um homomorfismo. Se $\overline{k}$ for par, já sabemos que $\varphi_{\overline{k}}$ é um isomorfismo, pois a identidade é um isomorfismo. Suponha $\overline{k}$ ímpar, neste caso, que

$$\varphi_{\overline{k}}(h_1 h_2) = (h_1 h_2)^{-1}$$

Como H é abeliano,

$$(h_1 h_2)^{-1} = (h_1)^{-1}(h_2)^{-1} = \varphi_{\overline{k}}(h_1)\varphi_{\overline{k}}(h_2)$$

Para qualquer $h \in H$, $\varphi_{\overline{k}}(h^{-1}) = h$, logo, $\varphi_{\overline{k}}$ é sobrejetora.
Sejam $h_1, h_2 \in H$, onde $\varphi_{\overline{k}}(h_1) = \varphi_{\overline{k}}(h_2)$. Temos que

$$\begin{aligned} \varphi_{\overline{k}}(h_1) &= \varphi_{\overline{k}}(h_2) \\ \implies h_1^{-1} &= h_2^{-1} \\ \implies h_1^{-1} h_2 &= 1 \\ \implies h_2 &= h_1 \end{aligned}$$

Logo, $\varphi_{\overline{k}}$ é um isomorfismo para qualquer $\overline{k} \in \mathbb{Z}_{2n}$. Portanto, temos que $H \rtimes_{\varphi} \mathbb{Z}_{2n}$ é um produto semidireto via φ, e a operação entre dois elementos deste grupo se dá da seguinte maneira:

$$(h_1, \overline{k_1})(h_2, \overline{k_2}) = \begin{cases} (h_1 h_2, \overline{k_1 k_2}), & \text{se } \overline{k_1} \text{ é par} \\ (h_1 h_2^{-1}, \overline{k_1 k_2}), & \text{se } \overline{k_1} \text{ é ímpar.} \end{cases}$$

Note que quando $\overline{k}$ é par, temos a mesma operação do produto direto.

Exemplo 2.36. Seja G um grupo qualquer e suponha que H seja um subgrupo do grupo de permutações S_n. Considere o produto direto generalizado

$$\underbrace{G \times G \times G \cdots \times G}_{n \; fatores}$$

Denotaremos este produto direto como G^n. Além disso, H irá permutar as entradas dos elementos de G^n assim como se comporta em n elementos como um subgrupo de S_n.
Vamos fazer a construção do produto semidireto $G^n \rtimes_{\varphi} H$.
Inicialmente, vejamos como é um elemento de H:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

Denotaremos α como um elemento de H, onde $\alpha(i)$ $i = 1, \ldots, n$ é a variação de 1 até n de acordo com a pemutação que α representa em H.
Considere a seguinte aplicação:

$$\varphi : H \to Aut(G^n)$$
$$\alpha \mapsto \varphi_{\alpha}$$

onde

$$\varphi_{\alpha}(g_1, g_2, \ldots, g_n) = (g_{\alpha(1)}, g_{\alpha(2)}, \ldots, g_{\alpha(n)})$$

A aplicação φ_α irá permutar as n entradas de um $(g_1, g_2, \ldots, g_n) \in G^n$ da mesma forma que permuta as entradas dos elementos do subgrupo H.
Para a construção do produto semidireto é necessário provar que:

1. φ é um homomorfismo
2. $\varphi_\alpha \in Aut(G^n)$ para cada $\alpha \in H$.

Para 1, vamos provar que $\varphi_{\alpha\circ\beta}(g) = (\varphi_\alpha \circ \varphi_\beta)(g)$
Sejam $\alpha, \beta \in H$

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

e

$$\beta = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta(1) & \beta(2) & \ldots & \beta(n) \end{pmatrix}$$

Temos que:

$$\begin{aligned} [\varphi_\alpha \circ \varphi_\beta](g_1, g_2, \ldots, g_n) &= \varphi_\alpha(\varphi_\beta(g_1, g_2, \ldots, g_n) \\ &= \varphi_\alpha(g_{\beta(1)}, g_{\beta(2)}, \cdots g_{\beta(n)}) \\ &= (g_{\alpha(\beta(1))}, g_{\alpha(\beta(2))}, \ldots, g_{\alpha(\beta(n))}) \\ &= (g_{(\alpha\circ\beta)(1)}, g_{(\alpha\circ\beta)(2)}, \ldots, g_{(\alpha\circ\beta)(n)}) \end{aligned}$$

que é justamente $\varphi_{\alpha\circ\beta}(g_1, g_2, \ldots, g_n)$. Assim conclui-se que φ é um homomorfismo.
Agora, precisamos provar que $\varphi_\alpha \in Aut(G^n)$. Para qualquer $\alpha \in H$ iniciaremos provando que φ_α é uma função bijetora.

Suponha $\varphi_\alpha(g_1, g_2, \ldots, g_n) = \varphi_\alpha(k_1, k_2, \ldots, k_n)$ com $g, k \in G$. Então

$$\begin{aligned} \varphi_\alpha(g_1, g_2, \ldots, g_n) &= \varphi_\alpha(k_1, k_2, \ldots, k_n) \\ \implies (g_{\alpha(1)}, g_{\alpha(2)}, \ldots, g_{\alpha(n)}) &= (k_{\alpha(1)}, k_{\alpha(2)}, \ldots, k_{\alpha(n)}) \end{aligned}$$

E como α é bijetora, portanto injetora, segue que

$$(g_1, g_2, \ldots, g_n) = (k_1, k_2, \ldots, k_n)$$

Agora, provaremos que dado $(k_1, k_2, \ldots, k_n) \in G$, existe $(g_1, g_2, \ldots, g_n) \in G$ tal que $\varphi_\alpha(g_1, g_2, \ldots, g_n) = (k_1, k_2, \ldots, k_n)$. Como α é uma função bijetora, existe uma inversa, seja ela β. Vamos provar que $(g_1, g_2, \ldots, g_n) = (k_{\beta(1)}, k_{\beta(2)}, \ldots, k_{\beta(n)})$:

$$\begin{aligned} \varphi_\alpha(g_1, g_2, \cdots, g_n) &= \varphi_\alpha(k_{\beta(1)}, k_{\beta(2)}, \ldots, k_{\beta(n)}) \\ &= (k_{\alpha\circ\beta(1)}, k_{\alpha\circ\beta(2)}, \ldots, k_{\alpha\circ\beta(n)}) \\ &= (k_1, k_2, \ldots, k_n) \end{aligned}$$

Logo, φ_α é uma função sobrejetora e portanto bijetora. Agora, falta mostrar que φ_α é um homomorfismo, isto é, que independente da ordem, permutação ou multiplicação, obtemos o mesmo elemento.
Note que

$$\varphi_\alpha(g \cdot k) = \varphi_\alpha(g_1k_1, g_2k_2 \ldots, g_nk_n)$$

Como $gk \in G$, podemos definir $gk = p$, e assim:

$$\begin{aligned} \varphi_\alpha(p) &= (p_{\alpha(1)}, p_{\alpha(2)}, \ldots, p_{\alpha(n)}) \\ &= (g_{\alpha(1)}k_{\alpha(1)}, g_{\alpha(2)}k_{\alpha(2)}, \ldots, g_{\alpha(n)}p_{\alpha(n)}) \\ &= \varphi_\alpha(g)\varphi_\alpha(k) \end{aligned}$$

Assim, φ_α é um homomorfismo bijetor de G^n em G^n, e portanto um automorfismo. Logo, a construção do produto semidireto $G^n \rtimes_\varphi H$ está concluída.
Sendo $\alpha, \beta \in H$ e $g^n, k^n \in G$, onde $g^n = (g_1, g_2, \ldots, g_n)$ e $k^n = (k_1, k_2, \ldots, k_n)$, a operação entre dois elementos de $G^n \rtimes_\varphi H$ se dará da seguinte maneira:

$$\begin{aligned}(g^n,\alpha)(k^n,\beta) &= (g^n\varphi_\alpha(k^n),\alpha\circ\beta)\\ &= ((g_1,g_2,\ldots,g_n)(k_{\alpha(1)},k_{\alpha(2)},k_{\alpha(n)}),\alpha\circ\beta)\\ &= ((g_1k_{\alpha(1)},g_2k_{\alpha(2)},\ldots,g_nk_{\alpha(n)}),\alpha\circ\beta)\end{aligned}$$

Vamos exemplificar este produto semidireto tomando $H = S^3$ e $G^n = \mathbb{R}^{*3} = \mathbb{R}^* \times \mathbb{R}^* \times \mathbb{R}^*$. Sejam $(a,b,c),(d,e,f) \in \mathbb{R}^{*3}$ e $\alpha,\beta \in S^3$, onde

$$\alpha = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

e

$$\beta = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

Logo,

$$\alpha\circ\beta = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

A operação entre dois elementos de $\mathbb{R}^{*3} \rtimes_\varphi S^3$ será:

$$\begin{aligned}((a,b,c),\alpha)((d,e,f),\beta) &= ((a,b,c)\varphi_\alpha((d,e,f)),\alpha\circ\beta)\\ &= ((a,b,c)(f,e,d),\alpha\circ\beta)\\ &= ((af,be,cd),\alpha\circ\beta)\end{aligned}$$

3 SEQUÊNCIAS EXATAS DE GRUPOS

A partir dos tópicos preliminares do Capítulo 2, é possível construir a ideia de sequências exatas. Uma sequência exata de grupos nada mais é do que uma sequência formada por grupos e entre eles homomorfismos que se relacionam entre si de uma forma específica. As sequências exatas curtas são um caso particular das sequências exatas, que serão apresentadas adiante.

Definição 3.1. Sejam H, G e K grupos, α e β homomorfismos. A sequência

$$H \xrightarrow{\alpha} G \xrightarrow{\beta} K$$

é chamada sequência exata em G se $Im(\alpha) = Ker(\beta)$.
Uma sequência exata de grupos pode ser formada por n ou até infinitos grupos, desde que os homomorfismos entre estes grupos satisfaçam a relação acima descrita. Uma sequência é exata quando ela é exata em todos os grupos que fazem parte dela.

A partir da definição acima, podemos observar alguns pontos importantes. Em uma sequência exata, temos que

$$Im(\alpha) = Ker(\beta)$$

Note que isto significa que para qualquer $h \in H$,

$$\beta(\alpha(h)) = 1$$

e, por outro lado, se $\beta(g) = 1$ segue que $g = \alpha(h)$ para algum h em H.

Suponha que

$$1 \xrightarrow{\varphi} H \xrightarrow{\alpha} G \xrightarrow{\beta} 1$$

seja uma sequência exata de grupos, onde 1 representa um grupo que é formado apenas por um elemento. Chamaremos este grupo de grupo unitário. Como esta sequência é exata, temos que

$$Im(\varphi) = Ker(\alpha) = 1$$

Logo, α é um homomorfismo injetor. Ainda,

$$Im(\alpha) = Ker(\beta) = G$$

Portanto α é um homomorfismo sobrejetor, e podemos concluir que α é um isomorfismo.
Ademais, se

$$1 \xrightarrow{\varphi} G \xrightarrow{\gamma} 1$$

é exata em G, segue que $Im(\varphi) = Ker(\gamma) = 1$, portanto, neste caso G é o grupo unitário.

Agora, considere a sequência exata abaixo:

$$1 \xrightarrow{\varphi} H \xrightarrow{\alpha} G \tag{2}$$

Como φ e α são homomorfismos, temos que

$$Ker(\alpha) = Im(\varphi)$$

Observe que φ deve ser o homomorfismo trivial, e assim,

$$Im(\varphi) = 1 = Ker(\alpha)$$

Por outro lado, se temos que α é injetora em (2) o núcleo de α será 1, e como φ é o homomorfismo trivial segue que $Im(\varphi) = Ker(\alpha)$. Portanto, dizer a sequência é exata em H é equivalente a dizer que α é uma função injetora.

Da mesma forma, se a sequência exata for do tipo

$$G \xrightarrow{\beta} K \xrightarrow{\gamma} 1 \tag{3}$$

obrigatoriamente

$$\gamma(k) = 1, \ \forall \ k \in K$$

e assim

$$K = Ker(\gamma) = Im(\beta)$$

fazendo de β um homomorfismo sobrejetor. Em contrapartida, se β for um homomorfismo sobrejetor a imagem de β será K, e como γ deve ser o homomorfismo trivial, segue que

$$Ker(\gamma) = K = Im(\beta)$$

Logo, a exatidão de (3) e a sobrejetividade de β são afirmações equivalentes.
As duas sequências exatas apresentadas em (2) e (3) são a base para definir sequências exatas curtas.

Definição 3.2. Uma sequência exata curta é uma sequência de grupos e homomorfismos do tipo

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$$

que é exata em H, G e K.

Perceba então que α é um homomorfismo injetor e β um homomorfismo sobrejetor.

Neste caso, não há necessidade de apontar os homomorfismos que "ligam" o grupo 1 nos outros, visto que temos apenas uma possibilidade em cada caso: no primeiro caso, o homomorfismo é o que leva unidade em unidade e no último caso, todos os elementos de K são levados na unidade, como apresentado anteriormente.

Observação 3.1. *Se a operação dos grupos for aditiva, podemos escolher representar o primeiro e o último grupos unitários por* 0.

A seguir, veremos alguns exemplos de sequências exatas curtas.

Exemplo 3.1. Considere a seguinte sequência exata curta

$$1 \longrightarrow SL_2(\mathbb{R}) \xrightarrow{\alpha} GL_2(\mathbb{R}) \xrightarrow{\beta} \mathbb{R}^* \longrightarrow 1$$

onde $SL_2(\mathbb{R})$ e $GL_2(\mathbb{R})$ são os grupos apresentados nos exemplos 2.15 e 2.8 e $\mathbb{R}^*$ é o grupo multiplicativo dos números reais não nulos. Lembre que $SL_2(\mathbb{R}) \leqslant GL_2(\mathbb{R})$. Neste caso, os homomorfismos entre os grupos serão definidos da seguinte maneira:

$$\begin{aligned} \alpha : SL_2(\mathbb{R}) &\to GL_2(\mathbb{R}) \\ M &\mapsto M \end{aligned}$$

Desta forma, α é uma função injetora. Na segunda parte da sequência,

$$\begin{aligned} \beta : GL_2(\mathbb{R}) &\to \mathbb{R}^* \\ M &\mapsto det(M) \end{aligned}$$

Temos que β é uma função sobrejetora pois, dado qualquer $x \in \mathbb{R}^*$, segue que existe uma matriz $M \in GL_2(\mathbb{R})$ da forma

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

com $\beta(M) = det(M) = x$, ou seja, β é sobrejetora.
Ainda,

$$Im(\alpha) = \{M \in SL_2 \subseteq GL_2(\mathbb{R}) : det(M) = 1\}$$

e

$$Ker(\beta) = \{M \in GL_2(\mathbb{R}) : det(M) = 1\}$$

Assim, $Im(\alpha) = Ker(\beta)$ e esta sequência configura uma sequência exata curta.

Exemplo 3.2. Seja $N \trianglelefteq G$. Podemos construir uma sequência exata curta da seguinte maneira:

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} G/N \longrightarrow 1$$

onde α é a função inclusão e β é a projeção canônica, como vimos no Exemplo 2.23. Assim, temos que

$$Ker(\beta) = N = Im(\alpha)$$

Nos dois próximos exemplos vamos definir sequências exatas curtas envolvendo produtos diretos e semidiretos.

Exemplo 3.3. Sejam H e K grupos. A partir deles, é possível construir uma sequência exata curta da seguinte maneira:

$$1 \longrightarrow H \xrightarrow{\alpha} H \times K \xrightarrow{\beta} K \longrightarrow 1$$

onde $\alpha(h) = (h, 1)$ e $\beta(h, k) = k$.
Vamos mostrar que esta é uma sequência exata curta de fato. Primeiramente, temos que α e β são homomorfismos, pois

$$\begin{aligned} \alpha(h_1h_2) &= (h_1h_2, 1) \\ &= (h_1, 1)(h_2, 1) \\ &= \alpha(h_1)\alpha(h_2) \end{aligned}$$

e ainda

$$\begin{aligned} \beta[(h_1, k_1)(h_2, k_2)] &= \beta(h_1h_2, k_1k_2) \\ &= k_1k_2 \\ &= \beta(h_1, k_1)\beta(h_2, k_2) \end{aligned}$$

É preciso garantir que $Im(\alpha) = Ker(\beta)$. Note que

$$\beta(\alpha(h)) = \beta(h, 1) = 1, \ \forall \ h \in H$$

Logo, temos que $Im(\alpha) \subset Ker(\beta)$. Por outro lado, temos

$$Ker(\beta) = \{(h,k) \in H \times K : \beta(h,k) = k = 1\}$$

ou seja, $Ker(\beta)$ é formado por par ordenado do tipo $(h,1)$, que são $\alpha(h)$. Sendo assim, $Ker(\beta) \subset Im(\alpha)$ e consequentemente, $Ker(\beta) = Im(\alpha)$.
Ainda é necessário mostrar que β é uma função sobrejetora e α é uma função injetora. Iniciaremos por β: suponha $k \in K$. Note que

$$\beta(1,k) = k, \ \forall \ k \in K$$

Logo, β é sobrejetora.
Dados $h_1, h_2 \in H$ com $h_1 \neq h_2$, temos que:

$$\alpha(h_1) = (h_1, 1)$$

e

$$\alpha(h_2) = (h_2, 1)$$

Como $h_1 \neq h_2$, certamente $(h_1,1) \neq (h_2,1)$. Logo, α é uma função injetora.

O próximo exemplo trata sobre a sequência exata curta usual envolvendo produtos semidiretos.

Exemplo 3.4. Sejam H e K grupos e $\varphi : K \to Aut(H)$ um homomorfismo. A partir do produto semidireto $H \rtimes_\varphi K$ podemos construir a seguinte sequência exata curta:

$$1 \longrightarrow H \xrightarrow{\alpha} H \rtimes_\varphi K \xrightarrow{\beta} K \longrightarrow 1$$

onde $\alpha(h) = (h,1)$ e $\beta(h,k) = k$.
Para mostrar que esta sequência é uma sequência exata curta, primeiramente precisamos provar que α e β são homomorfismos.

Temos que α e β são um homomorfismos, pois

$$\begin{aligned} \alpha(h_1h_2) &= (h_1h_2, 1) \\ &= (h_1, 1)(h_2, 1) \\ &= \alpha(h_1)\alpha(h_2) \end{aligned}$$

e

$$\begin{aligned} \beta[(h_1k_1)(h_2k_2)] &= \beta(h_1\varphi_{k_1}(h_2), k_1k_2) \\ &= k_1k_2 \\ &= \beta(h_1, k_1)\beta(h_2, k_2) \end{aligned}$$

As provas da imagem ser igual ao núcleo, injetividade de α e sobrejetividade de β são idênticas às do exemplo anterior.

Definição 3.3. Sejam

$$1 \longrightarrow H_1 \xrightarrow{\alpha} G_1 \xrightarrow{\beta} K_1 \longrightarrow 1$$

e

$$1 \longrightarrow H_2 \xrightarrow{\gamma} G_2 \xrightarrow{\varphi} K_2 \longrightarrow 1$$

sequências exatas curtas. Considere o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\alpha} & G_1 & \xrightarrow{\beta} & K_1 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \lambda} & & \\ 1 & \longrightarrow & H_2 & \xrightarrow{\gamma} & G_2 & \xrightarrow{\varphi} & K_2 & \longrightarrow & 1 \end{array}$$

onde δ, θ e λ são isomorfismos. Dizemos que este diagrama é comutativo se

$$\theta \circ \alpha = \gamma \circ \delta$$

e

$$\lambda \circ \beta = \varphi \circ \theta$$

Quando duas sequências exatas se encaixam em tal diagrama, dizemos que elas são isomorfas. Quando sabemos que o diagrama é comutativo é possível "caminhar" pelos grupos por meio das funções, usando a composição, de modo que para chegar em determinado grupo podemos compor funções de várias direções, e sempre chegar no mesmo elemento.

A partir de uma sequência exata curta qualquer, da forma

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$$

sempre podemos escrever uma sequência exata curta isomorfa a esta usando um grupo quociente, mesmo que H não seja um subgrupo normal de G e mesmo se K não puder ser escrito como G/H. No próximo teorema veremos como esta segunda sequência é obtida.

Teorema 3.1. *Toda sequência exata curta da forma*

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1 \tag{4}$$

é isomorfa a uma sequência exata curta do tipo

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \longrightarrow 1 \tag{5}$$

onde N é um subgrupo normal de G.

Demonstração. Mostraremos os isomorfismos necessários para obter a sequência (5). Como α é uma função injetora, podemos definir um isomorfismo a partir de α entre H e $\alpha(H)$. Note que como (4) é exata, $\alpha(H) = Ker(\beta) \subseteq G$, e como $Im(\beta) = K$, pelo Teorema 2.1 existe um isomorfismo

$$\overline{\beta} : K \to G/Ker(\beta)$$

Desta forma, a partir de uma sequência exata curta genérica do tipo (4), obtemos uma sequência exata curta da forma (5), onde $N = \alpha(H) = Ker(\beta)$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \alpha\downarrow & & id\downarrow & & \overline{\beta}\downarrow & & \\ 1 & \longrightarrow & \alpha(H) & \xrightarrow{i} & G & \xrightarrow{\pi} & G/Ker(\beta) & \longrightarrow & 1 \end{array}$$

onde as funções nas flechas verticais são isomorfismos e os homomorfismos na sequência exata curta inferior são análogos aos apresentados no Exemplo 3.2. □

Quando temos que $N \trianglelefteq G$, e conhecemos N e G/N, de um modo geral podemos não saber dizer quem é G. Mesmo que dois grupos não sejam isomorfos, eles podem ter subgrupos normais isomorfos com grupos quocientes isomorfos, como mostraremos nos exemplos seguintes.

Exemplo 3.5. Os Exemplos 2.11 e 2.10 nos apresentaram os grupos D_4 e Q_8. O grupo D_4 não é isomorfo ao grupo Q_8, pois eles possuem quantidades diferentes de elementos de ordem 2, contradizendo o Teorema 2.2. Mas

$$\{r_0, r_2\} \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

e ainda

$$D_4/\{r_0, r_2\} \cong Q_8/\{\pm 1\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

como vimos nos Exemplos 2.32 e 2.33.
Assim, é possível construir as seguintes sequências exatas curtas:

$$1 \longrightarrow \{r_0, r_2\} \xrightarrow{\alpha} D_4 \xrightarrow{\beta} D_4/\{r_0, r_2\} \longrightarrow 1$$

e

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\varphi} Q_8 \xrightarrow{\gamma} Q_8/\{\pm 1\} \longrightarrow 1$$

Note que os grupos ocupando as segundas e quartas posições da sequência são isomorfos, mesmo os grupos do meio não o sendo.

Exemplo 3.6. Sejam as seguintes sequências exatas curtas:

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

e

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/8\mathbb{Z} \xrightarrow{\gamma} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Neste exemplo podemos observar que é possível que tenhamos os mesmos segundos e quartos grupos compondo as sequências, com grupos não isomorfos no meio. Na primeira sequência, temos que

$$\alpha(\overline{x}) = (\overline{x}, \overline{0})$$

e

$$\beta(\overline{x}, \overline{y}) = \overline{y}$$

Na segunda sequência, $\varphi(\overline{x}) = \overline{x}$ e

$$\gamma(\overline{x}) = \begin{cases} \overline{0}, & \text{se } x \text{ é par} \\ \overline{1}, & \text{se } x \text{ é ímpar} \end{cases}$$

Os homomorfismos implícitos são os triviais. Note que pelo fato dos grupos serem aditivos, usamos o 0 para representar os grupos das pontas.

3.1 PRODUTOS DIRETOS E SEMIDIRETOS

Dados dois grupos H e K, sempre podemos criar uma sequência exata curta utilizando o seu produto direto, basta seguir a receita do Exemplo 3.3. Mas, analisando a segunda sequência do Exemplo 3.6, perceba que nem toda sequência é obtida assim.

Da mesma forma, se seguirmos os passos do Exemplo 3.4, será possível criar uma sequência exata curta com o produto semidireto de tais grupos. Mas isso não significa que toda sequência exata é construída dessa maneira, conforme o próximo exemplo nos mostra.

Exemplo 3.7. Na sequência exata curta

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\alpha} Q_8 \xrightarrow{\beta} Q_8/\{\pm 1\} \longrightarrow 1$$

temos que Q_8 não é isomorfo ao produto semidireto de $\{\pm 1\}$ e $Q_8/\{\pm 1\}$, pois neste há mais de um elemento de ordem 2. De fato, temos que $Aut(\{\pm 1\}) = id$, pois este é o único isomorfismo possível entre o grupo $\{\pm 1\}$ e ele mesmo. Desta forma, o produto semidireto $\{\pm 1\} \rtimes_{\varphi} Q_8/\{\pm 1\}$ é na verdade, o produto direto. Note que,

$$(1, \{\pm 1\})^2 = (1, 1)$$

e

$$(-1, \{\pm 1\})^2 = (1, 1)$$

Assim, segue que $\{\pm 1\} \times Q_8/\{\pm 1\}$ possui dois elementos de ordem 2, enquanto Q_8 tem apenas um.

Os dois próximos teoremas, que são o objetivo deste trabalho, tratam de critérios para que uma sequência exata curta seja isomorfa a uma sequência que envolve produtos diretos e semidiretos, a partir de algumas condições impostas aos homomorfismos que compõem as sequências.

Teorema 3.2. *Seja* $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ *uma sequência exata curta. As seguintes afirmações são equivalentes:*
(1) Existe um homomorfismo $\alpha' : G \to H$ *tal que* $\alpha'(\alpha(h)) = h$, $\forall\, h \in H$.
(2) Existe um isomorfismo $\theta : G \to H \times K$ *tal que o diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

comuta, onde a linha inferior é a sequência exata curta para o produto direto, como no Exemplo 3.3.

Demonstração. (1) $\implies$ (2)
Vamos definir θ da seguinte maneira:

$$\begin{aligned} \theta : G &\to H \times K \\ g &\mapsto (\alpha'(g), \beta(g)) \end{aligned}$$

Inicialmente, provaremos que θ é um isomorfismo. Como α' e β são homomorfismos, segue que θ é um homomorfismo. De fato, sejam $g_1, g_2 \in G$:

$$\begin{aligned} \theta(g_1 g_2) &= (\alpha'(g_1 g_2), \beta(g_1 g_2)) \\ &= (\alpha'(g_1)\alpha'(g_2), \beta(g_1)\beta(g_2)) \\ &= (\alpha'(g_1), \beta(g_1))(\alpha'(g_2), \beta(g_2)) \\ &= \theta(g_1)\theta(g_2) \end{aligned}$$

Logo, falta provar que θ é uma aplicação bijetora. Começaremos pela injetividade. Seja $g \in Ker(\theta)$. Logo $\theta(g) = (1, 1)$ e, daí, $\alpha'(g) = 1$ e $\beta(g) = 1$. Sabemos que essa sequência é exata em G, se $\beta(g) = 1$ então $g = \alpha(h)$ para algum h em H, pois $Im(\alpha) = Ker(\beta)$. Logo, temos que

$$1 = \alpha'(g) = \alpha'(\alpha(h)) = h$$

e então

$$g = \alpha(h) = \alpha(1) = 1$$

Isto nos diz que $Ker(\theta) = 1$ logo, θ é injetora.
Para mostrar que θ é sobrejetora, devemos mostrar que para qualquer $(h, k) \in H \times K$, existe $g \in G$ tal que $\theta(g) = (h, k)$.
Seja $(h, k) \in H \times K$. Como β é sobrejetora, para todo $k \in K$, existe $g \in G$ de modo que $\beta(g) = k$. A partir disto, usando β, precisamos

mostrar qual é o g que satisfaz estas condições.
Do fato de que $Im(\alpha) = ker(\beta)$, segue que

$$\beta(g\alpha(x)) = \beta(g)\beta(\alpha(x)) = \beta(g) = k$$

Assim, para todo $x \in H$,

$$\begin{aligned} \theta(g\alpha(x)) &= (\alpha'(g\alpha(x)), \beta(g\alpha(x)) \\ &= (\alpha'(g)\alpha'(\alpha(x)), k) \\ &= (\alpha'(g)x, k) \end{aligned}$$

Agora, é preciso definir x para que $\alpha'(g)x = h$. Seja $x = \alpha'(g)^{-1}h$. Temos que

$$\begin{aligned} \alpha'(g)x &= \alpha'(g)\alpha'(g)^{-1}h \\ &= h \end{aligned}$$

Portanto, $\theta(g\alpha(x)) = (h, k)$ e θ é sobrejetora. Uma vez que a prova de θ ser um isomorfismo foi concluída, falta verificar se o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

comuta.
Vamos analisar o primeiro quadrado do diagrama:

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} \\ H & \longrightarrow & H \times K \end{array}$$

Considere $h \in H$. Partindo de H, localizado no canto superior esquerdo, podemos chegar em $H \times K$ de duas maneiras. Indo para a direita, tem-se que:

$$h \overset{\alpha}{\mapsto} \alpha(h) \overset{\theta}{\mapsto} (\alpha'(\alpha(h)), \beta(\alpha(h)) = (h, 1)$$

Pelo outro caminho,

$$h \overset{id}{\mapsto} h \mapsto (h, 1)$$

Analisando o segundo quadrado:

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle id} \\ H \times K & \longrightarrow & K \end{array}$$

Seja $g \in G$. A partir de G, se seguirmos pela direita, temos que:

$$g \overset{\beta}{\mapsto} \beta(g) \overset{id}{\mapsto} \beta(g)$$

Se seguirmos a flecha que vai para baixo, segue que

$$g \overset{\theta}{\mapsto} (\alpha'(g), \beta(g)) \mapsto \beta(g)$$

Logo, o diagrama comuta.

(2) $\implies$ (1)

Suponha que exista um isomorfismo $\theta : G \to H \times K$ de modo que o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & {\scriptstyle id}\downarrow & & {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

comute. Queremos provar que existe um homomorfismo α' tal que $\alpha'(\alpha(h)) = h$ para qualquer $h \in H$.

Considere o segundo quadrado do diagrama:

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle id} \\ H \times K & \longrightarrow & K \end{array}$$

Sendo $g \in G$, temos que

$$g \overset{\beta}{\mapsto} \beta(g) \overset{id}{\mapsto} \beta(g)$$

Pela comutatividade do diagrama, sabemos que $\theta(g)$ tem como segunda coordenada $\beta(g)$, então precisamos saber qual é a primeira. Denote por $\alpha'(g)$ a primeira coordenada e assim

$$\theta(g) = (\alpha'(g), \beta(g))$$

Logo, $\alpha' : G \to H$ é uma função e como θ e β são homomorfismos, α' é um homomorfismo, pois

$$\begin{aligned} \theta(g_1 g_2) &= \theta(g_1)\theta(g_2) \\ \implies (\alpha'(g_1 g_2), \beta(g_1 g_2)) &= (\alpha'(g_1), \beta(g_1))(\alpha'(g_2), \beta(g_2)) \\ \implies (\alpha'(g_1 g_2), \beta(g_1 g_2)) &= (\alpha'(g_1)\alpha'(g_2), \beta(g_1)\beta(g_2)) \\ \implies \alpha'(g_1 g_2) &= \alpha'(g_1)\alpha'(g_2) \end{aligned}$$

Para provar que $\alpha'(\alpha(h)) = h \,\forall\, h \in H$, considere o primeiro quadrado do diagrama:

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \theta} \\ H & \longrightarrow & H \times K \end{array}$$

Se seguirmos a partir do grupo H localizado no canto superior esquerdo, seguindo pra baixo temos que

$$h \overset{id}{\mapsto} h \mapsto (h, 1)$$

e, se seguirmos para direita primeiro,

$$h \overset{\alpha}{\mapsto} \alpha(h) \overset{\theta}{\mapsto} (\alpha'(\alpha(h)), \beta(\alpha(h))$$

e consequentemente, $\alpha'(\alpha(h)) = h$ para todo $h \in H$ e segue o resultado.

□

Vamos aplicar o Teorema 3.2 no próximo exemplo.

Exemplo 3.8. Considere o grupo multiplicativo $\mathbb{Z}_8{}^*$ e seu subgrupo $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Seja

$$1 \longrightarrow \mathbb{Z}_2 \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbb{Z}_2 \longrightarrow 1$$

uma sequência exata de grupos, onde

$$\begin{array}{cccc} \alpha\colon & \mathbb{Z}_2 & \to & G \\ & \overline{0} & \mapsto & \overline{1} \\ & \overline{1} & \mapsto & \overline{3} \end{array} \qquad \begin{array}{cccc} \beta\colon & G & \to & \mathbb{Z}_2 \\ & \overline{1} & \mapsto & \overline{0} \\ & \overline{3} & \mapsto & \overline{0} \\ & \overline{5} & \mapsto & \overline{1} \\ & \overline{7} & \mapsto & \overline{1} \end{array}$$

Note que α é um homomorfismo injetor, β é um homomorfismo sobrejetor e ainda que

$$Im(\alpha) = \{\overline{1}, \overline{3}\} = Ker(\beta)$$

Desta forma, podemos definir o homomorfismo

$$\begin{aligned} \alpha' : G &\to \mathbb{Z}_2 \\ \overline{1} &\mapsto \overline{0} \\ \overline{3} &\mapsto \overline{1} \\ \overline{5} &\mapsto \overline{1} \\ \overline{7} &\mapsto \overline{0} \end{aligned}$$

Perceba que $\alpha'(\alpha(h)) = h$ para qualquer $h \in \mathbb{Z}_2$. Portanto, pelo Teorema 3.2 temos que $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ e podemos escrever o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}_2 & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & \mathbb{Z}_2 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 1 \end{array}$$

onde θ é um isomorfismo.

No próximo teorema veremos quais são as condições para uma sequência exata curta ser isomorfa a uma sequência exata curta que envolve produto semidireto.

Teorema 3.3. *Seja* $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ *uma sequência exata curta. As seguintes afirmações são equivalentes:*
(1) Existe um homomorfismo $\beta' : K \to G$ *tal que* $\beta(\beta'(k)) = k$, $\forall\, k \in K$.
(2) Existe um homomorfismo $\varphi : K \to Aut(H)$ *e um isomorfismo* $\theta : G \to H \rtimes_\varphi K$ *tal que o diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

comuta, onde a linha inferior é a sequência exata curta usual para o produto semidireto, como no Exemplo 3.4.

Demonstração. (1) $\implies$ (2)
A partir do homomorfismo β' vamos criar um homomorfismo φ de K em $Aut(H)$ e o isomorfismo $\theta : G \to H \rtimes_\varphi K$.
Sejam $k \in K$ e $h \in H$. Vamos verificar que $\beta'(k)\alpha(h)\beta'(k^{-1})$ está no núcleo de β:

$$\begin{aligned} \beta[\beta'(k)\alpha(h)\beta'(k^{-1})] &= \beta(\beta'(k))\beta(\alpha(h))\beta(\beta'(k^{-1})) \\ &= k1k^{-1} \\ &= kk^{-1} \\ &= 1 \end{aligned}$$

Logo, temos que esta conjugação pertence ao núcleo de β, e isto significa que esse elemento pode ser escrito como $\alpha(h')$, para algum

$h' \in H$, devido ao fato de que $Im(\alpha) = Ker(\beta)$. Ainda, h' é único devido a injetividade de α. Note que h' é determinado por H e por K, e podemos escrever h' como $\varphi_k(h)$ onde, então, $\varphi_k(h)$ denotará um elemento único de H, de modo que

$$\beta'(k)\alpha(h)\beta'(k)^{-1} = \alpha(h') \tag{6}$$

onde

$$h' = \varphi_k(h)$$

Como $\varphi_k(h) \in H$, obtemos a aplicação $\varphi_k : H \to H$, e devemos mostrar que $\varphi_k \in Aut(H)$, e que $k \mapsto \varphi_k$ é um homomorfismo de K em $Aut(H)$.
Fazendo $k = 1$ em (6):

$$\alpha(h) = \alpha(\varphi_1(h))$$

então, como α é injetora,

$$h = \varphi_1(h)$$

Precisamos garantir que $\varphi_k : H \to H$ seja um homomorfismo para cada $k \in K$.
Considere $h_1, h_2 \in H$. Temos que $\varphi_k(h_1h_2)$ pode ser caracterizado pela equação

$$\beta'(k)\alpha(h_1h_2)\beta'(k)^{-1} = \alpha(\varphi_k(h_1h_2))$$

Mas,

$$\begin{aligned}
\beta'(k)\alpha(h_1h_2)\beta'(k)^{-1} &= \beta'(k)\alpha(h_1)\alpha(h_2)\beta'(k)^{-1} \\
&= \beta'(k)\alpha(h_1)\beta'(k)^{-1}\beta'(k)\alpha(h_2)\beta'(k)^{-1} \\
&= \alpha(\varphi_k(h_1))\alpha(\varphi_k(h_2)) \\
&= \alpha[\varphi_k(h_1)\varphi_k(h_2)]
\end{aligned}$$

Portanto,

$$\alpha(\varphi_k(h_1h_2)) = \alpha[\varphi_k(h_1)\varphi_k(h_2)]$$

e como α é injetora, temos que

$$\varphi_k(h_1h_2) = \varphi_k(h_1)\varphi_k(h_2)$$

Logo, $\varphi_k : H \to H$ é um homomorfismo.
Agora, precisamos provar que φ é um homomorfismo, ou seja, que $\varphi_{k_1k_2} = \varphi_{k_1} \circ \varphi_{k_2}$.
Seja $h \in H$. Temos que

$$\beta'(k_1k_2)\alpha(h)\beta'(k_1k_2)^{-1} = \alpha(\varphi_{k_1k_2}(h))$$

Por outro lado, se

$$\begin{aligned}\beta'(k_1k_2)\alpha(h)\beta'(k_1k_2)^{-1} &= \beta'(k_1)\beta'(k_2)\alpha(h)\beta'(k_2)^{-1}\beta'(k_1)^{-1} \\ &= \beta'(k_1)\alpha(\varphi_{k_2}(h)\beta'(k_1)^{-1} \\ &= \alpha(\varphi_{k_1}(\varphi_{k_2}(h)))\end{aligned}$$

E então

$$\begin{aligned}\varphi_{k_1k_2}(h) &= \alpha(\varphi_{k_1}(\varphi_{k_2}(h))) \\ \implies \varphi_{k_1k_2} &= \varphi_{k_1} \circ \varphi_{k_2}\end{aligned}$$

Note que φ_k é bijetora, pois é inversível com inversa $\varphi_{k^{-1}}$:

$$\varphi_k \circ \varphi_{k^{-1}} = \varphi_1$$

e ainda

$$\varphi_{k^{-1}} \circ \varphi_k = \varphi_1$$

Portanto, $\varphi_k \in Aut(H)$ e $k \mapsto \varphi_k$ é um homomorfismo

$$K \to Aut(H)$$

Logo é possível construir o produto semidireto $H \rtimes_\varphi K$.
O próximo passo é mostrar um isomorfismo

$$\theta : G \to H \rtimes_\varphi K$$

e o caminho que será tomado é mostrar que existe

$$\gamma : H \rtimes_\varphi K \to G$$

onde γ é um isomorfismo, e θ será a inversa de γ.
Sejam $h_1, h_2 \in H$, $k_1, k_2 \in K$ e defina γ da seguinte maneira:

$$\gamma(h, k) = \alpha(h)\beta'(k)$$

Temos que γ é um homomorfismo, pois

$$\begin{aligned}
\gamma[(h_1, k_1)(h_2, k_2)] &= \gamma(h_1\varphi_{k_1}(h_2), k_1k_2) \\
&= \alpha(h_1\varphi_{k_1}(h_2))\beta'(k_1k_2) \\
&= \alpha(h_1)\alpha(\varphi_{k_1}(h_2))\beta'(k_1)\beta'(k_2) \\
&= \alpha(h_1)\beta'(k_1)\alpha(h_2)\beta'(k_1)^{-1}\beta'(k_1)\beta'(k_2) \\
&= \alpha(h_1)\beta'(k_1)\alpha(h_2)\beta'(k_2) \\
&= \gamma(h_1, k_1)\gamma(h_2, k_2)
\end{aligned}$$

Para mostrar que γ é injetiva, suponha $\gamma(h, k) = 1$. Assim,

$$\alpha(h)\beta'(k) = 1$$

Aplicando β nos dois lados desta igualdade, segue que

$$\begin{aligned}
\alpha(h)\beta'(k) &= 1 \\
\implies \beta(\alpha(h)\beta'(k)) &= \beta(1) \\
\implies \beta(\alpha(h))\beta(\beta'(k)) &= \beta(1) \\
\implies k &= \beta(1) \\
\implies k &= 1
\end{aligned}$$

Então,

$$\alpha(h)1 = 1 \implies h = 1$$

pela injetividade de α. E com isso, conclui-se que γ é uma aplicação injetora.

Em seguida, provaremos que γ é sobrejetora.

Seja $g \in G$. Temos que mostrar que para qualquer $g \in G$, existe $(h.k) \in H \rtimes_\varphi K$ tais que $\gamma(h,k) = \alpha(h)\beta'(k) = g$.

Analisando

$$\alpha(h)\beta'(k) = g,$$

se aplicarmos β dos dois lados da igualdade temos:

$$\begin{aligned} \alpha(h)\beta'(k) &= g \\ \implies \beta(\alpha(h)\beta'(k)) &= \beta(g) \\ \implies \beta(\alpha(h))\beta(\beta'(k)) &= \beta(g) \\ \implies k &= \beta(g) \end{aligned}$$

Desta forma, vamos tomar $k = \beta(g)$ e precisamos somente encontrar um h que satisfaça

$$\alpha(h) = g\beta'(k^{-1}) = g\beta'(\beta(g^{-1}))$$

Como a imagem de α é igual ao núcleo de β, basta verificar se o elemento $g\beta'(\beta(g^{-1}))$ pertence ao núcleo de β:

$$\begin{aligned} \beta[g\beta'(\beta(g^{-1}))] &= \beta(g)\beta(\beta'(\beta(g^{-1})) \\ &= \beta(g)\beta(g^{-1}) \\ &= 1 \end{aligned}$$

Portanto, $g\beta'(\beta(g^{-1})) \in Ker(\beta)$, ou seja, $g\beta'(\beta(g^{-1})) \in Im(\alpha)$, logo, pode ser escrito como $\alpha(h)$ para um $h \in H$. Finalmente, temos que γ é um isomorfismo e pode-se definir $\theta = \gamma^{-1}$.

Em seguida, vamos provar que o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

comuta. Para isso, usaremos o "diagrama inverso" ao invés do seu sentido original. Por que podemos trabalhar com o diagrama inverso? Seja f o homomorfismo para produto semidireto apresentado no Exemplo 3.4. Mostrar que o diagrama

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \theta} \\ H & \xrightarrow{f} & H \rtimes_\varphi K \end{array}$$

comuta, é o mesmo que mostrar que

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ \uparrow{\scriptstyle id} & & \uparrow{\scriptstyle \gamma} \\ H & \xrightarrow{f} & H \rtimes_\varphi K \end{array}$$

comuta, pois de acordo com o diagrama original, temos que:

$$\begin{aligned} \theta \circ \alpha &= f \circ id \\ \implies \gamma \circ (\theta \circ \alpha) &= \gamma \circ (f \circ id) \\ \implies \alpha &= \gamma \circ f \\ \implies \alpha \circ id &= \gamma \circ f \end{aligned}$$

Logo, seja $h \in H$. No primeiro quadrado

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ \uparrow{\scriptstyle id} & & \uparrow{\scriptstyle \gamma} \\ H & \longrightarrow & H \rtimes_\varphi K \end{array}$$

se seguirmos a partir do grupo H localizado no canto inferior esquerdo, segue que

$$h \overset{id}{\mapsto} h \overset{\alpha}{\mapsto} \alpha(h)$$

e se, partindo do mesmo H seguirmos a seta para a direita, temos

$$h \mapsto (h,1) \overset{\gamma}{\mapsto} \gamma(h,1) = \alpha(h)\beta'(1) = \alpha(h)$$

Considere o segundo quadrado do diagrama:

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle\gamma}\uparrow & & \uparrow{\scriptstyle id} \\ H \rtimes_\varphi K & \longrightarrow & K \end{array}$$

Seja $(h,k) \in H \rtimes_\varphi K$. Seguindo pela seta vertical:

$$(h,k) \overset{\gamma}{\mapsto} \alpha(h)\beta'(k) \overset{\beta}{\mapsto} \beta(\alpha(h)\beta'(k)) = \beta(\alpha(h))\beta(\beta'(k)) = k$$

e por outro lado,

$$(h,k) \mapsto k \overset{id}{\mapsto} k$$

Logo, o diagrama é comutativo.

(2) $\implies$ (1)

Suponha que exista um isomorfismo $\theta : G \to H \rtimes_\varphi K$, um homomorfismo $\varphi : K \to Aut(H)$ e que o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & {\scriptstyle id}\downarrow & & {\scriptstyle\theta}\downarrow & & {\scriptstyle id}\downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

seja comutativo. Queremos mostrar que existe um homomorfismo $\beta' : K \to G$ tal que $\beta(\beta'(k)) = k \,\forall\, k \in K$.

A motivação para esta parte da demonstração é pensar em γ, pois no caso (1) $\implies$ (2), vimos que

$$\gamma(h,k) = \alpha(h)\beta'(k) \implies \gamma(1,k) = \beta'(k)$$

Logo, podemos pensar em $\beta' : K \to G$ definido da seguinte maneira:

$$\beta'(k) = \theta^{-1}(1,k)$$

Note que $k \mapsto (1, k)$ é um homomorfismo, e sendo θ um isomorfismo, θ^{-1} também o é. Assim, β' é um homomorfismo.
Como o diagrama

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle \theta^{-1}}\uparrow & & \uparrow{\scriptstyle id} \\ H \rtimes_{\varphi} K & \longrightarrow & K \end{array}$$

é comutativo, segue que $\beta(\beta'(k)) = \beta(\theta^{-1}(1, k)) = k$. □

Definição 3.4. As sequências exatas curtas

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$$

que satisfazem as condições do Teorema 3.2 são denominadas sequências exatas curtas que cindem à direita, enquanto as sequências que satisfazem as condições do Teorema 3.3 são ditas sequências exatas curtas que cindem à esquerda.

No inglês, as sequências exatas curtas que satisfazem as condições do Teorema 3.2 são definidas como *split sequences*. Caso a sequência seja como a do Teorema 3.3, ela é dita *half-split*.

Em seguida, vamos ver um exemplo de uma sequência exata curta que cinde à esquerda, usando a ideia de construção dos homomorfismos e isomorfismos do Teorema 3.3.

Exemplo 3.9. Seja

$$1 \longrightarrow \mathbb{Z}_4 \xrightarrow{\alpha} D_4 \xrightarrow{\beta} \mathbb{Z}_2 \longrightarrow 1$$

uma sequência exata curta. Primeiramente, definiremos os homomorfismos que compõem esta sequência.

$$\begin{array}{cccc} \alpha: & \mathbb{Z}_4 & \to & D_4 \\ & \overline{0} & \mapsto & r_0 \\ & \overline{1} & \mapsto & r_1 \\ & \overline{2} & \mapsto & r_2 \\ & \overline{3} & \mapsto & r_3 \end{array} \qquad \begin{array}{cccc} \beta: & D_4 & \to & \mathbb{Z}_2 \\ & r_0 & \mapsto & \overline{0} \\ & r_1 & \mapsto & \overline{0} \\ & r_2 & \mapsto & \overline{0} \\ & r_3 & \mapsto & \overline{0} \\ & s & \mapsto & \overline{1} \\ & r_1 \circ s & \mapsto & \overline{1} \\ & r_2 \circ s & \mapsto & \overline{1} \\ & r_3 \circ s & \mapsto & \overline{1} \end{array}$$

Perceba que $Im(\alpha) = Ker(\beta)$. Agora, vamos definir β', onde

$$\begin{aligned} \beta' : \mathbb{Z}_2 &\to D_4 \\ \overline{0} &\mapsto r_0 \\ \overline{1} &\mapsto s \end{aligned}$$

Note que $\beta(\beta'(h)) = h \ \forall \ h \in \mathbb{Z}_2$. O Teorema 3.3 nos garante que existe um homomorfismo

$$\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_4)$$

Podemos nos perguntar quem seria φ e, pela Equação (6) do Teorema 3.3, obtemos a resposta:

$$\beta'(\overline{0})\alpha(h)\beta'(\overline{0})^{-1} = \alpha(\varphi_{\overline{0}}(h)) \implies \varphi_{\overline{0}}(h) = h$$

e

$$\begin{aligned} \alpha(\varphi_{\overline{1}}(h)) = \beta'(\overline{1})\alpha(h)\beta'(\overline{1})^{-1} &= s\alpha(h)s^{-1} \\ &= \alpha(h)^{-1}ss^{-1} \\ &= \alpha(h)^{-1} \\ &= \alpha(h^{-1}) \\ \implies \varphi_{\overline{1}}(h) &= h^{-1} \end{aligned}$$

Portanto, $D_4 \simeq \mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_2$.

4 CONSIDERAÇÕES FINAIS

Neste trabalho pude revisar conceitos da teoria de anéis e principalmente da teoria de grupos que fizeram parte da minha formação acadêmica.

O objetivo era estudar os aspectos elementares das sequências exatas de grupos a fim de compreender, demonstrar e aplicar os dois teoremas finais do trabalho.

De todas as disciplinas que fazem parte do currículo de licenciatura em matemática, certamente as Álgebras foram as que mais me interessaram, pela maneira como seus conceitos são construídos.

Um próximo passo seria nos aprofundarmos no estudo de sequências exatas, curtas ou não, com o intuito de conhecer a homologia e a cohomologia.

REFERÊNCIAS

[1] Keith Conrad. *Splitting of short exact sequences for groups*. 2018. Disp. em: `https://tinyurl.com/w8debmmc` (acesso em 16/02/2021).

[2] David S. Dummit & Richard M. Foote. *Abstract algebra*. 3ª ed. Hoboken, 2004.

[3] John B Fraleigh. *A first course in abstract algebra*. Pearson Education India, 2003.

[4] Hygino H. Domingues e Gelson Lezzi. *Álgebra moderna*. 5ª ed. São Paulo: Saraiva: Saraiva educação, 2018.

[5] Adilson Gonçalves. *Introdução à álgebra*. 5ª ed. Rio de Janeiro: IMPA, 2013.

[6] Gregory T Lee. *Abstract algebra: An introductory course*. Springer, 2018.